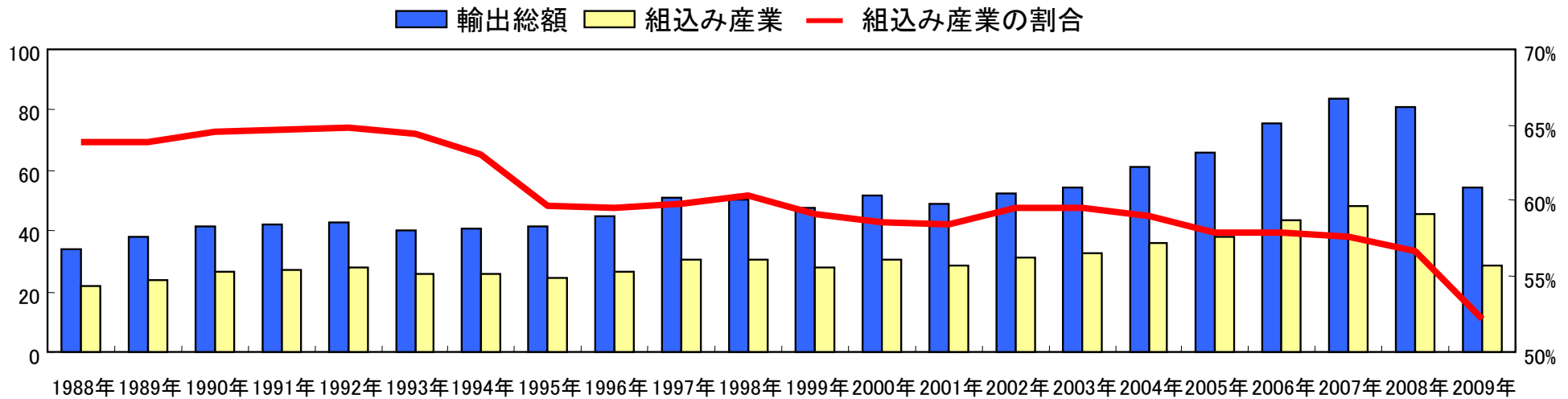
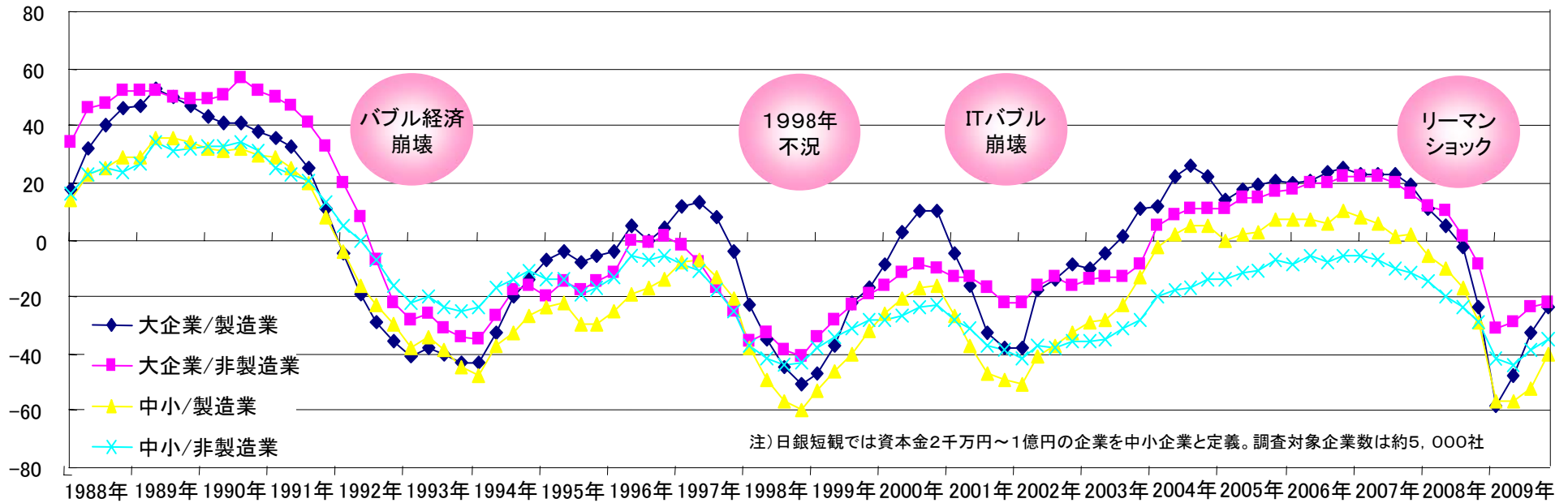
組込み産業イノベーションの方向性

独立行政法人　情報処理推進機構　ソフトウェア・エンジニアリング・センター
統合系プロジェクト＆組込み系プロジェクト　サブリーダー

工学博士　田丸　喜一郎

日銀短観と組込み産業の輸出額の推移

主要地域別の輸出に占める組込み製品

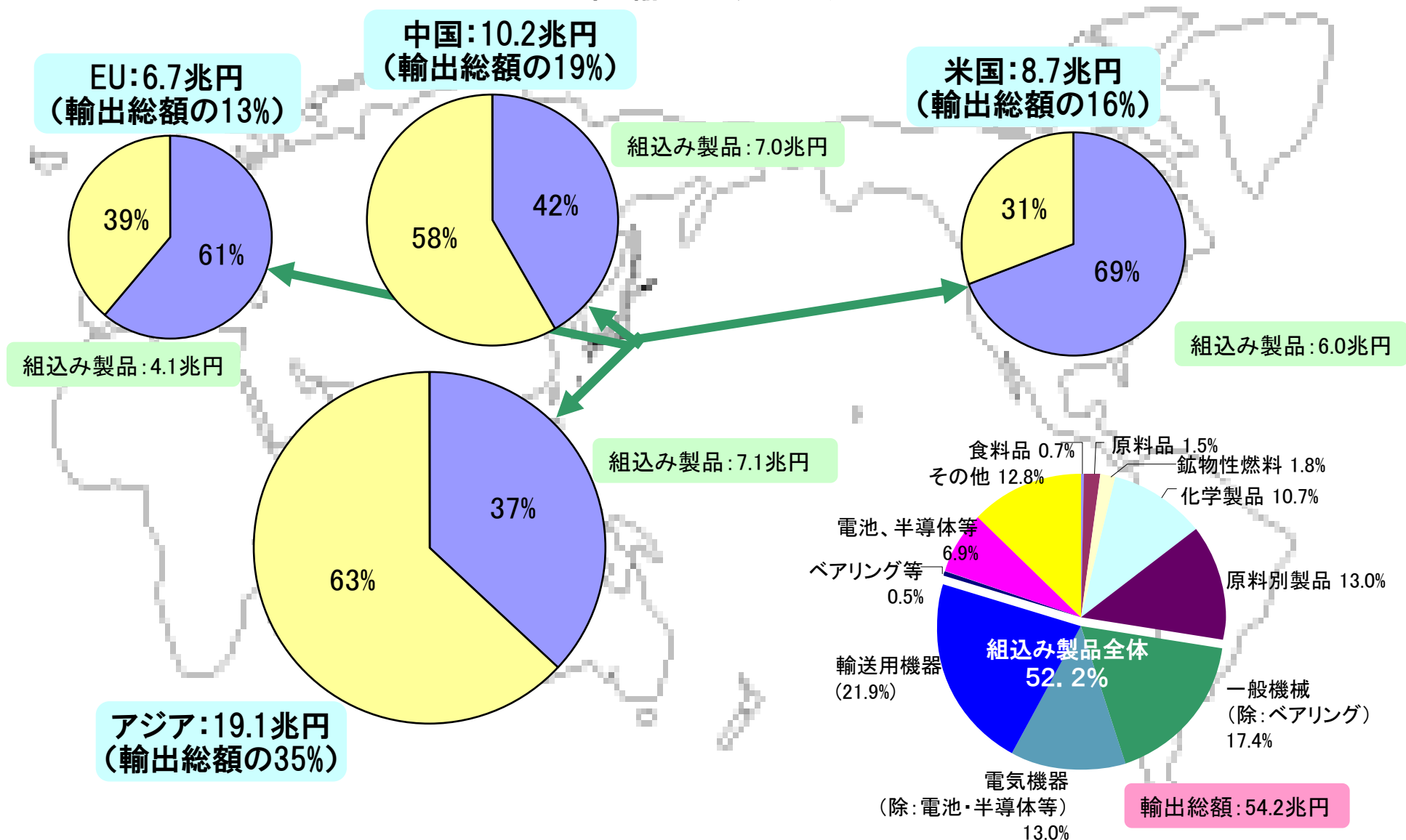
2009年　輸出総額:54.2兆円

EU:6.7兆円
(輸出総額の13%)
39%
61%
組込み製品:4.1兆円

中国:10.2兆円
(輸出総額の19%)
58%
42%
組込み製品:7.0兆円

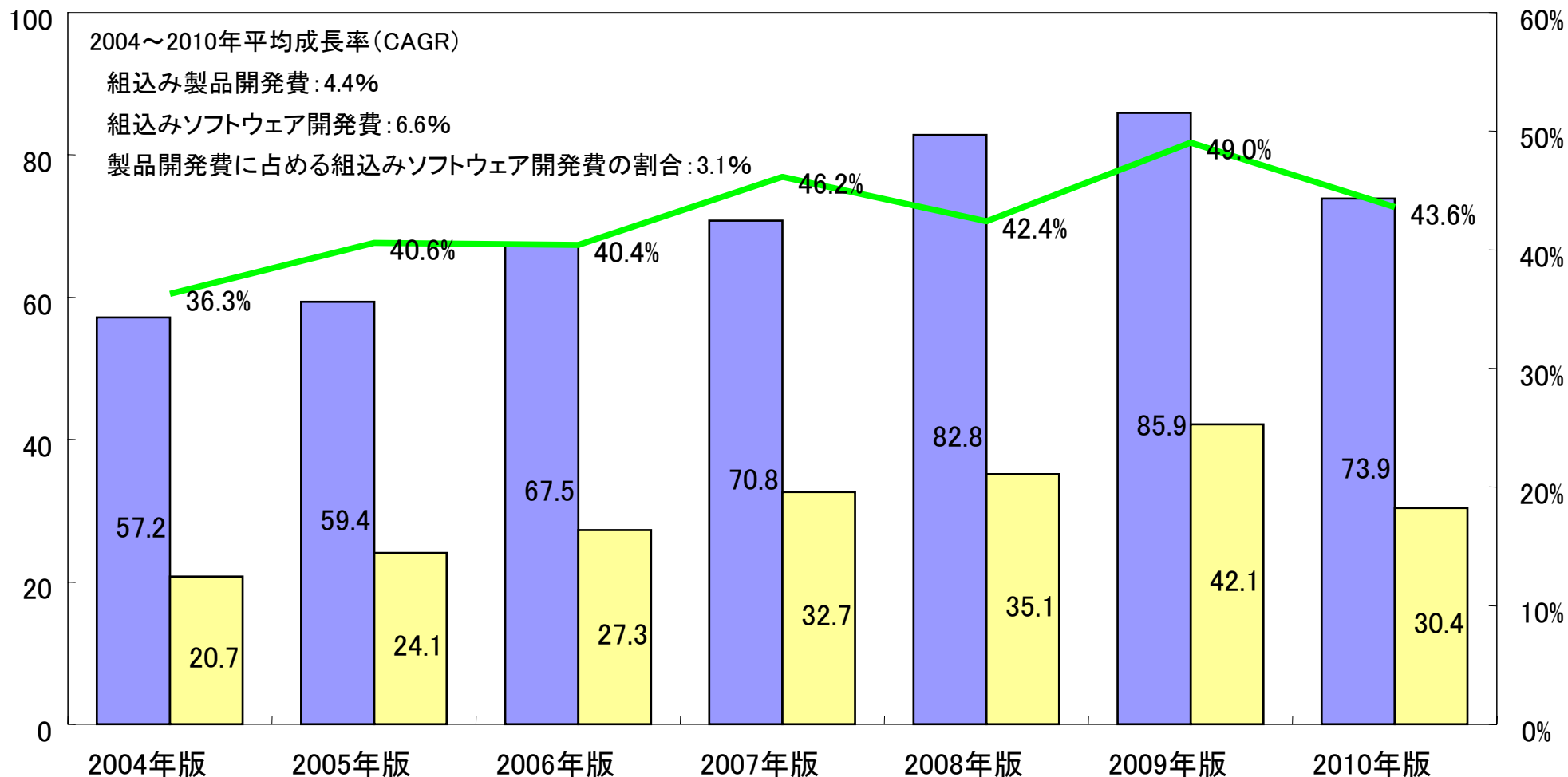
米国:8.7兆円
(輸出総額の16%)
31%
69%
組込み製品:6.0兆円

アジア:19.1兆円
(輸出総額の35%)
63%
37%
組込み製品:7.1兆円

食料品 0.7%
原料品 1.5%
鉱物性燃料 1.8%
化学製品 10.7%
その他 12.8%
電池、半導体等 6.9%
ベアリング等 0.5%
原料別製品 13.0%
組込み製品全体 52.2%
輸送用機器 (21.9%)
一般機械 (除:ベアリング) 17.4%
電気機器 (除:電池･半導体等) 13.0%
輸出総額:54.2兆円

組込み製品開発費と組込みソフトウェア開発費の推移

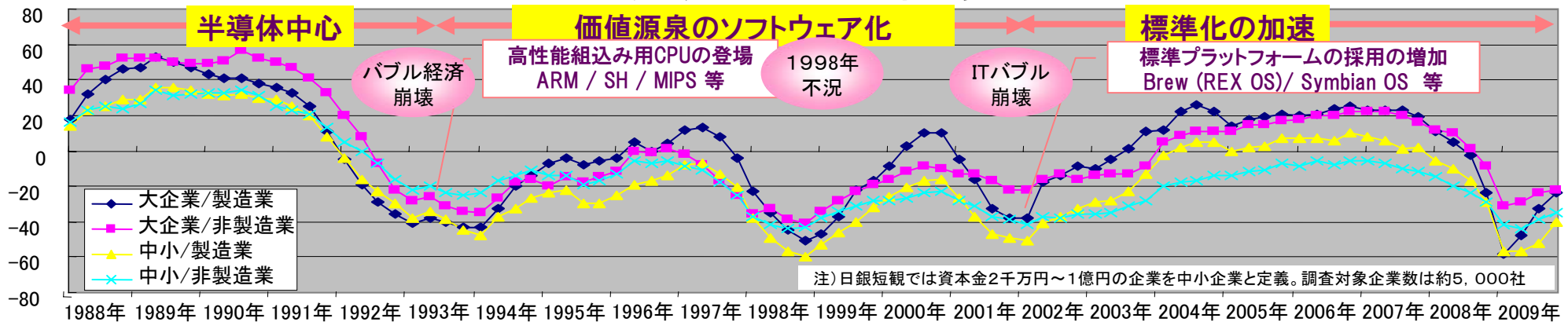
組込み製品開発費（1,000億円） 組込みソフトウェア開発費（1,000億円） 製品開発費に占める組込みソフトウェア開発費の割合

2004～2010年平均成長率（CAGR）
組込み製品開発費：4.4%
組込みソフトウェア開発費：6.6%
製品開発費に占める組込みソフトウェア開発費の割合：3.1%

	組込み製品開発費（1,000億円）	組込みソフトウェア開発費（1,000億円）	製品開発費に占める組込みソフトウェア開発費の割合
2004年版	57.2	20.7	36.3%
2005年版	59.4	24.1	40.6%
2006年版	67.5	27.3	40.4%
2007年版	70.8	32.7	46.2%
2008年版	82.8	35.1	42.4%
2009年版	85.9	42.1	49.0%
2010年版	73.9	30.4	43.6%

（社）日本機械工業連合会（平成20年度生産額実績統計）

経済危機が促す組込み産業の変革

- 1992年、2001年の経済危機には、それぞれ、組込み産業に変革が起きた
- 「100年に1度の経済危機」の景気回復時を支える組込み産業における革新は？

日銀短観と組込み産業の変化

ご参考：半導体ベンダランキングの推移（出典：ガートナーデータクエスト）

Rank	1971年	1981年	1986年	1989年	1992年	1993年	1994年	1995年	1996年	1997年	1998年	1999年	2000年	2001年	2002年	2003年	2004年	2005年	2006年	2007年
1	TI	TI	NEC	NEC	Intel	Intel	Intel	Intel	Intel	Intel	Intel	Intel	Intel	Intel	Intel	Intel	Intel	Intel	Intel	Intel
2	Motorola	Motorola	日立	東芝	NEC	NEC	NEC	NEC	NEC	NEC	NEC	NEC	東芝	東芝	Samsung	Samsung	Samsung	Samsung	Samsung	Samsung
3	FCI゛	NEC	東芝	日立	東芝	Motorola	東芝	東芝	東芝	Motorola	Motorola	東芝	NEC	STMicro	東芝	ルネサス	TI	TI	TI	東芝
4	NS	日立	Motorola	Motorola	Motorola	東芝	Motorola	日立	Motorola	TI	東芝	Samsung	Samsung	Samsung	STMicro	TI	ルネサス	東芝	Infineon	TI
5	ｼｸﾞﾈﾃｨｯｸｽ	東芝	TI	富士通	日立	日立	日立	Motorola	TI	東芝	TI	TI	TI	TI	TI	東芝	Infineon	STMicro	STMicro	Infineon
6	NEC	NS	PHILIPS	TI	TI	TI	TI	Samsung	日立	日立	日立	Motorola	STMicro	NEC	NEC	STMicro	STMicro	ルネサス	東芝	STMicro
7	日立	Intel	富士通	三菱電機	富士通	Samsung	Samsung	TI	Samsung	Samsung	Samsung	日立	Motorola	Motorola	Infineon	Infineon	東芝	Infineon	Hynix	Hynix
8	AMI	松下電子	松下電子	Intel	三菱電機	富士通	富士通	富士通	富士通	富士通	PHILIPS	STMicro	日立	日立	Motorola	NECエレ	NECエレ	NECエレ	ルネサス	ルネサス
9	三菱電機	PHILIPS	三菱電機	松下電子	PHILIPS	三菱電機	三菱電機	三菱電機	三菱電機	PHILIPS	STMicro	PHILIPS	Infineon	Infineon	PHILIPS	Motorola	PHILIPS	Hynix	AMD	AMD
10	ﾕﾆﾄﾛｰﾄﾞ	FCI	Intel	PHILIPS	松下電子	IBM	PHILIPS	Hyundai	PHILIPS	STMicro	Infineon	Infineon	Micron	PHILIPS	日立	PHILIPS	Freescale	AMD	NXP	NXP

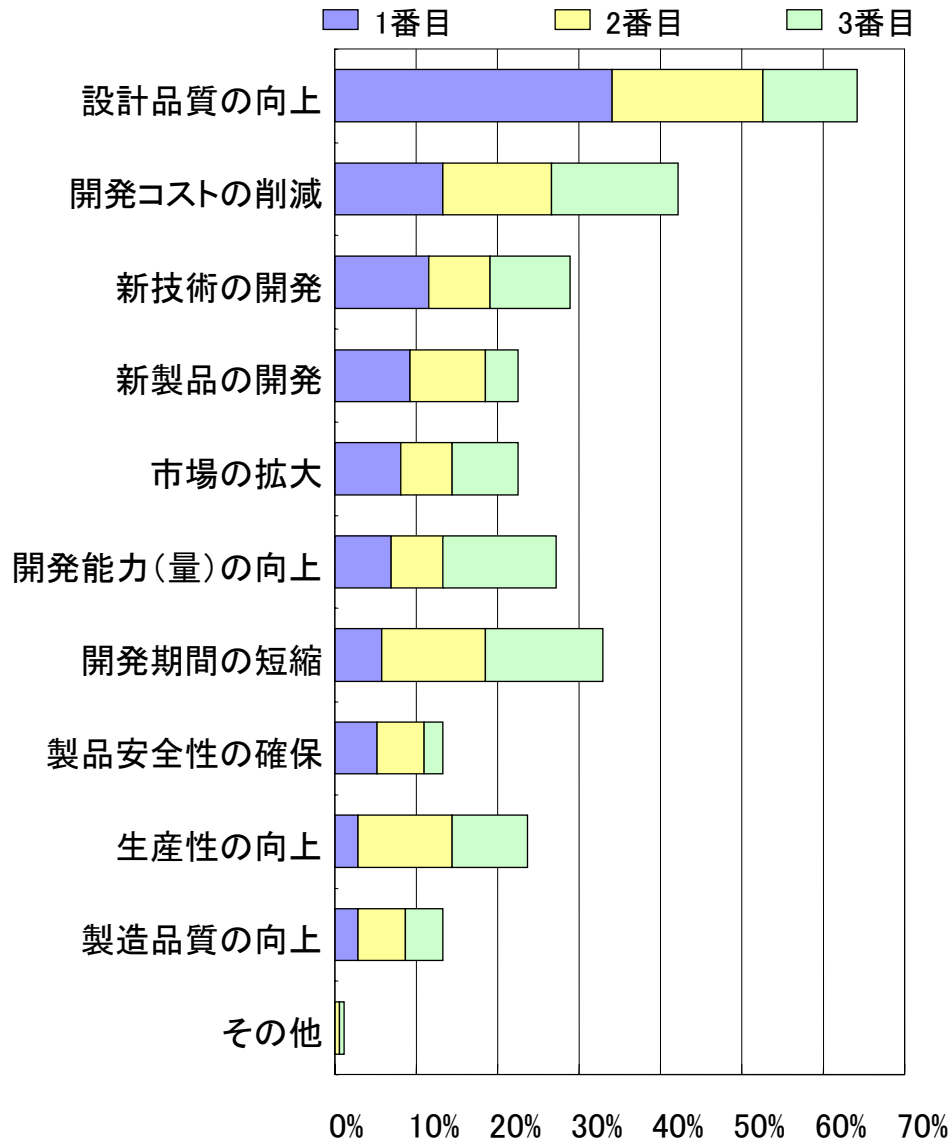
組込みソフトウェア開発の課題

事業責任者

2010年版

1番目　2番目　3番目

設計品質の向上
開発コストの削減
新技術の開発
新製品の開発
市場の拡大
開発能力(量)の向上
開発期間の短縮
製品安全性の確保
生産性の向上
製造品質の向上
その他

0%　10%　20%　30%　40%　50%　60%　70%

2007～2010年の1番目の課題の推移

2007	2008	2009	2010
設計品質	設計品質	設計品質	設計品質
新製品	新製品	開発期間	開発コスト
開発期間	開発期間	生産性	新技術
開発能力	開発能力	開発コスト	新製品
生産性	開発コスト	開発能力	市場拡大
開発コスト	生産性	新技術	開発能力
市場拡大	市場拡大	製造品質	開発期間
新技術	新技術	新製品	製品安全
製品安全	製品安全	市場拡大	生産性
製造品質	製造品質	製品安全	製造品質

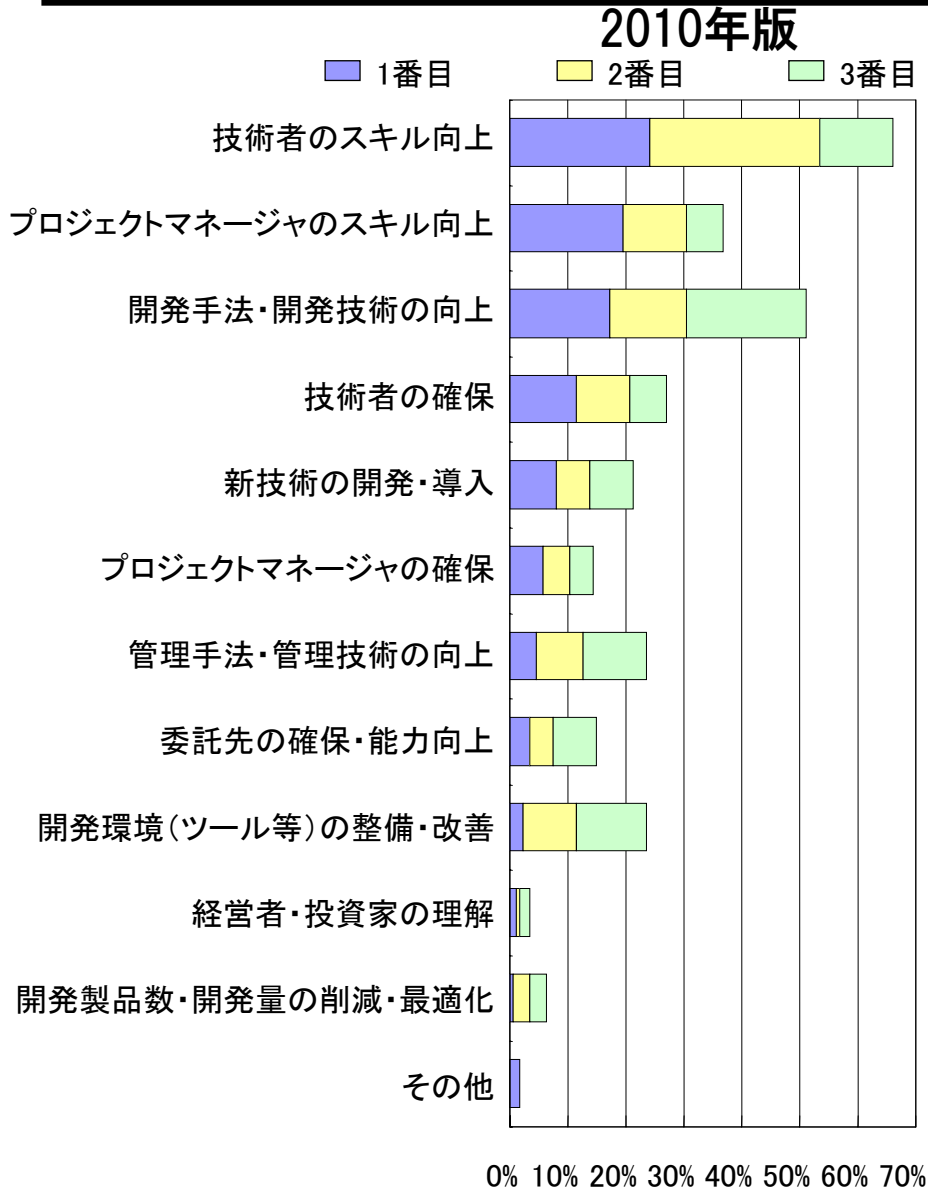
出典:2010年版　組込みソフトウェア産業実態調査

組込みソフトウェア開発課題解決の有効手段

2010年版

1番目　2番目　3番目

技術者のスキル向上
プロジェクトマネージャのスキル向上
開発手法・開発技術の向上
技術者の確保
新技術の開発・導入
プロジェクトマネージャの確保
管理手法・管理技術の向上
委託先の確保・能力向上
開発環境（ツール等）の整備・改善
経営者・投資家の理解
開発製品数・開発量の削減・最適化
その他

0% 10% 20% 30% 40% 50% 60% 70%

2007～2010年の1番目の解決手段の推移

2007	2008	2009	2010
技術者スキル向上	技術者スキル向上	技術者スキル向上	技術者スキル向上
技術者の確保	技術者の確保	PMのスキル向上	PMのスキル向上
PMのスキル向上	PMのスキル向上	開発技術の向上	開発技術の向上
開発技術の向上	開発技術の向上	PMの確保	技術者の確保
PMの確保	PMの確保	技術者の確保	新技術開発・導入
管理技術の向上	管理技術の向上	管理技術の向上	PMの確保
新技術開発・導入	新技術開発・導入	新技術開発・導入	管理技術の向上
開発環境の整備	開発環境の整備	開発製品数最適化	委託先の確保
開発製品数最適化	委託先の確保	開発環境の整備	開発環境の整備
経営者の理解	経営者の理解	委託先の確保	経営者の理解

出典：2010年版　組込みソフトウェア産業実態調査

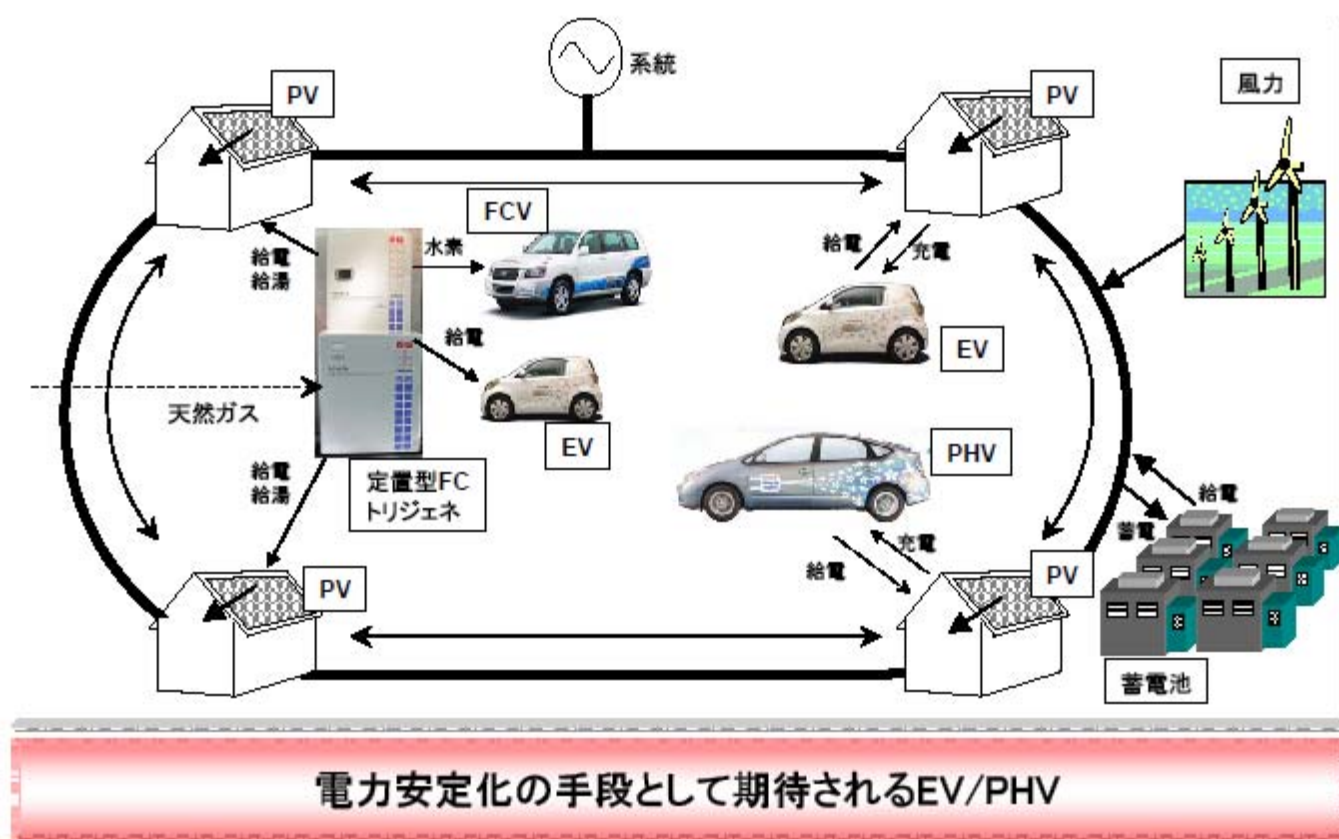
組込み産業イノベーションの方向性

- 経済危機の今が産業構造改革の最適なタイミング
  - 必然的に構造改革が要求される
    - コスト低減
    - 開発効率向上 & 品質確保
- 経済危機からの脱却時の組込みソフトウェアの浮上地点
  - 組込み製品のパラダイムシフト
    - 自動車は「エンジン」から「モータ」へ
    - エネルギーは「使う」から「作る」へ
  - 組込み製品の利用環境の変化
    - スタンドアロン型製品からネットワーク型製品へ
    - 社会インフラと連携する統合システム化
  - 組込みソフトウェアの開発スタイルの変化
    - 上流工程中心のソフトウェア開発
    - コーディングレスのソフトウェア開発
- 組込み産業イノベーションの方向性
  - 開発スタイルの革新
    - 開発効率と製品品質の両立のための「摺合せ型開発と組合せ型開発の適切な使い分け」
    - 「人材のみに頼る開発」から「組込みソフトウェア開発ツールを活用する開発」への移行
    - 「コーディングレス開発」に対応した上流工程技術者の育成・強化
  - 産業構造の革新
    - 産業界の枠組みを超えた「産業間連携」「人的ネットワーク形成」の構築
    - 開発コストの低減のための「競争領域と非競争領域を意識した水平分業化」

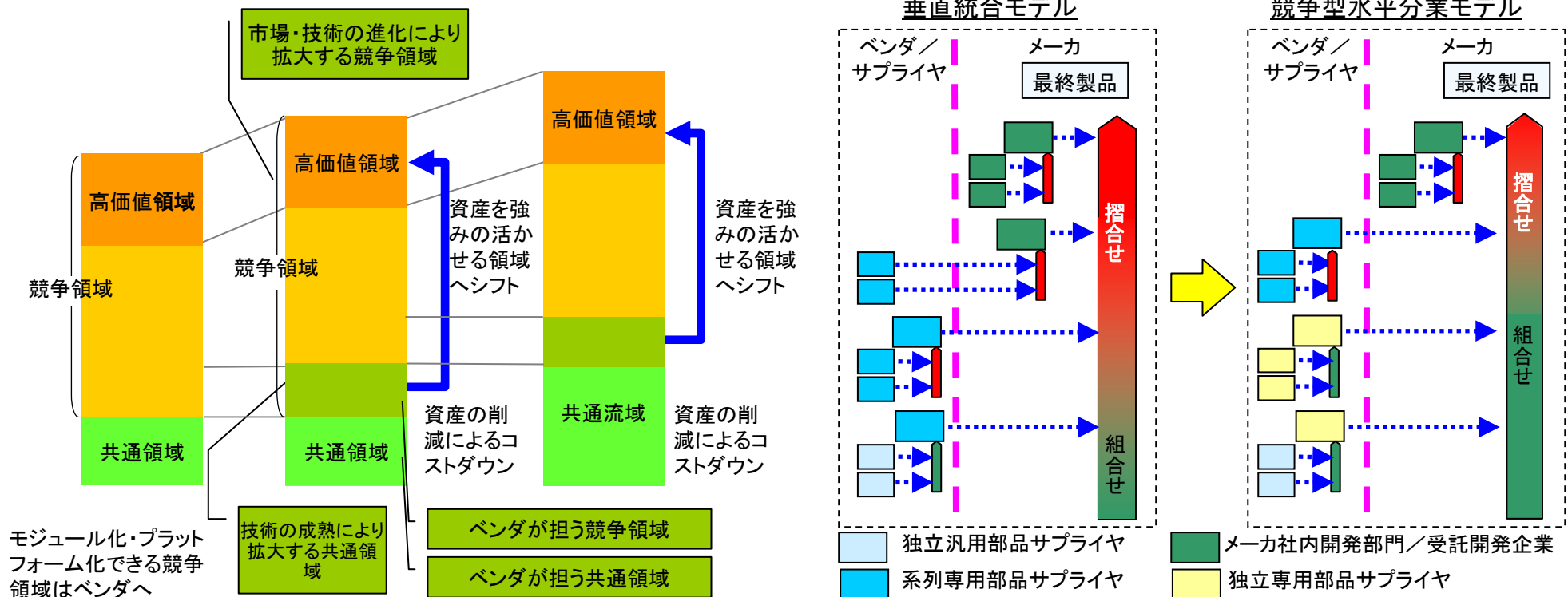
動力源がモータに変わり、電力インフラとつながる自動車

スマートグリッド概念の中のEV/PHV

系統
PV
PV
風力
FCV
水素
給電
給湯
給電
充電
EV
給電
天然ガス
EV
PHV
給電
給湯
定置型FC
トリジェネ
給電
蓄電
充電
給電
PV
PV
蓄電池

電力安定化の手段として期待されるEV/PHV

出典： トヨタ自動車畔柳部長のESEC2010基調講演より抜粋

競争領域と共通領域を意識した水平分業化

- 組込みシステムメーカは強みを活かせる「高価値領域」へ開発資源を集中、「共通領域」は部品化・ツール化して部品ベンダ、ツールベンダにシフト
- 「擂合せ型開発」と「組合せ型開発」を適切に使い分け、水平分業化により開発コストを削減
- ベンダは実装中心の受託開発サービスの提供から部品・ツール製品の提供、システム設計中心の受託開発サービスの提供へシフト

「人材のみに頼る開発」から「開発ツールを活用する開発」へ

- 我が国における開発ツールの使用率は、海外に比べ低水準
- 特に、開発の上流工程で使用するツール、テスト工程で使用するツール、管理系ツールの使用率が低い
- 「ツール購入・使用の理由」として、「品質確保」、「開発期間短縮」、「開発費削減」等が挙げられており、ツールの使用がQCD向上に繋がると認識

海外との比較

日本　海外平均　海外に対する日本の使用比率

平均使用率　比率

100%　80%　60%　40%　20%　0%

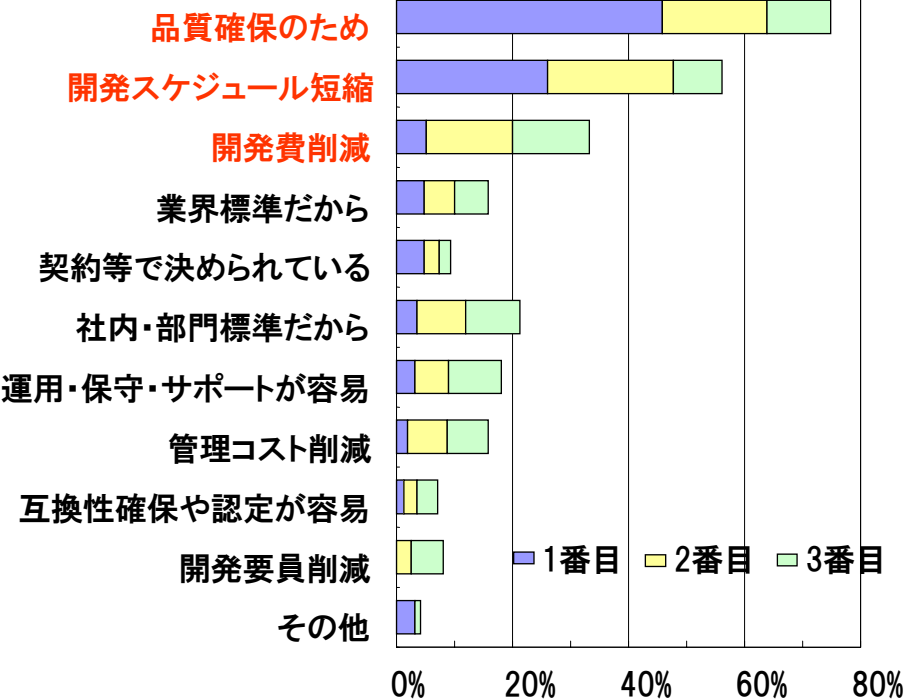
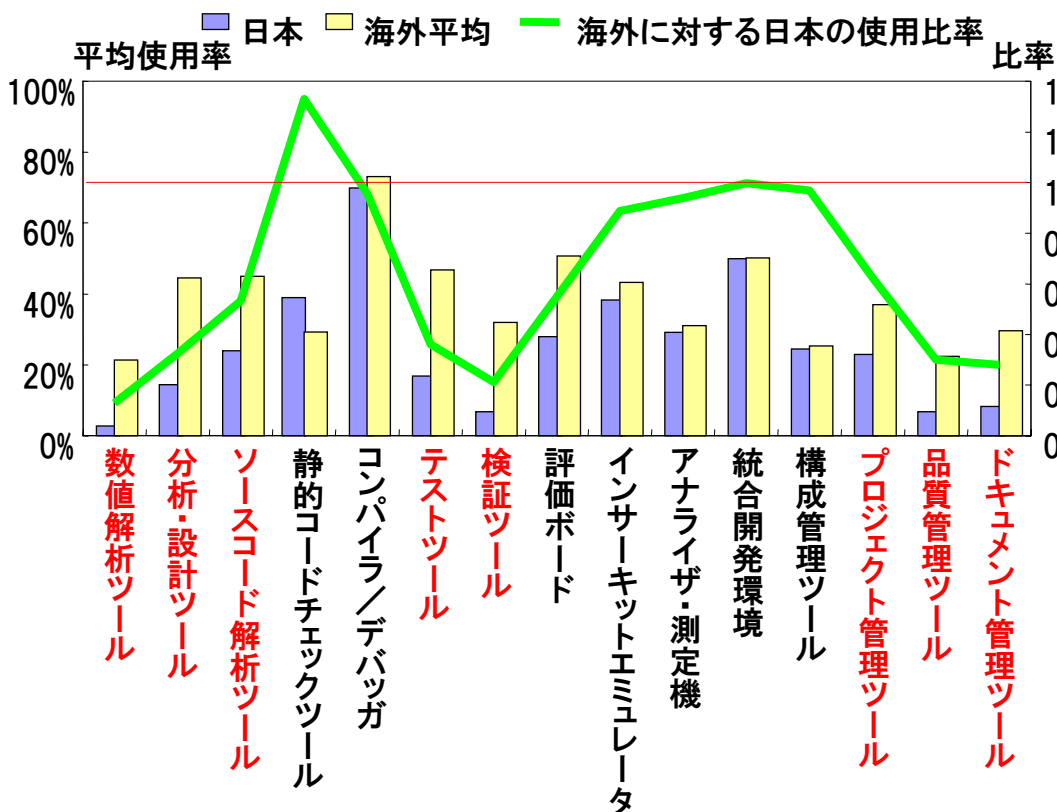
1.4　1.2　1.0　0.8　0.6　0.4　0.2　0.0

数値解析ツール　分析・設計ツール　ソースコード解析ツール　静的コードチェックツール　コンパイラ／デバッガ　テストツール　検証ツール　評価ボード　インサーキットエミュレータ　アナライザ・測定機　統合開発環境　構成管理ツール　プロジェクト管理ツール　品質管理ツール　ドキュメント管理ツール

ツール購入・使用の理由

品質確保のため
開発スケジュール短縮
開発費削減
業界標準だから
契約等で決められている
社内・部門標準だから
運用・保守・サポートが容易
管理コスト削減
互換性確保や認定が容易
開発要員削減
その他

1番目　2番目　3番目

0%　20%　40%　60%　80%

出典：2009年版　組込みソフトウェア産業実態調査

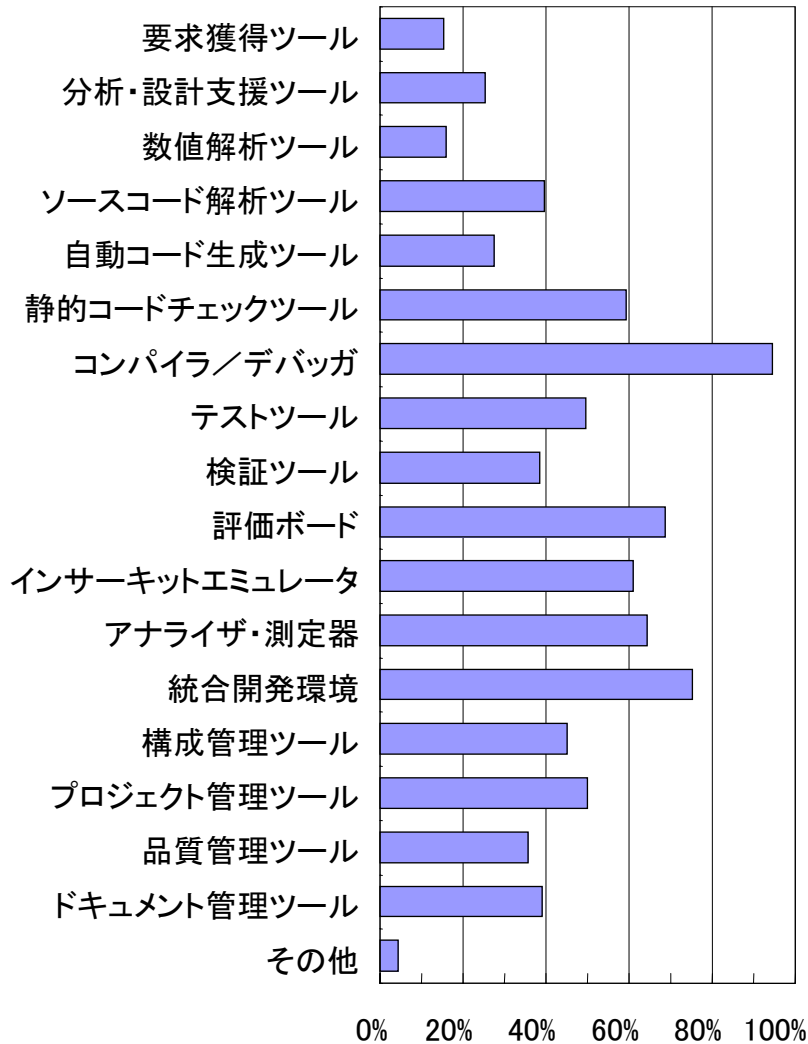
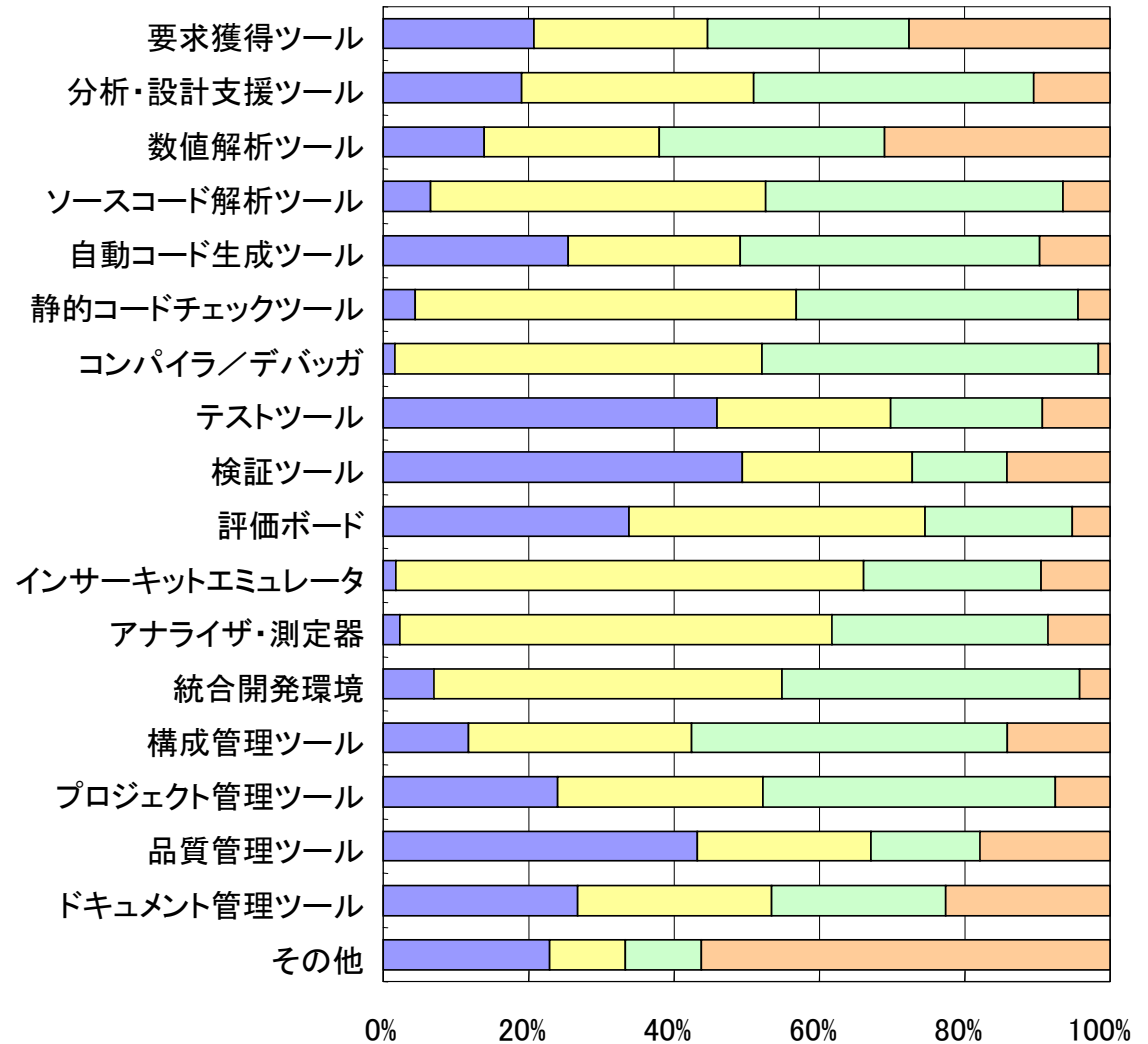
ツールの利用状況(内製・日本製・海外製)

プロジェクト責任者

利用率

内製 / 日本製 / 海外製 / 製造者不明

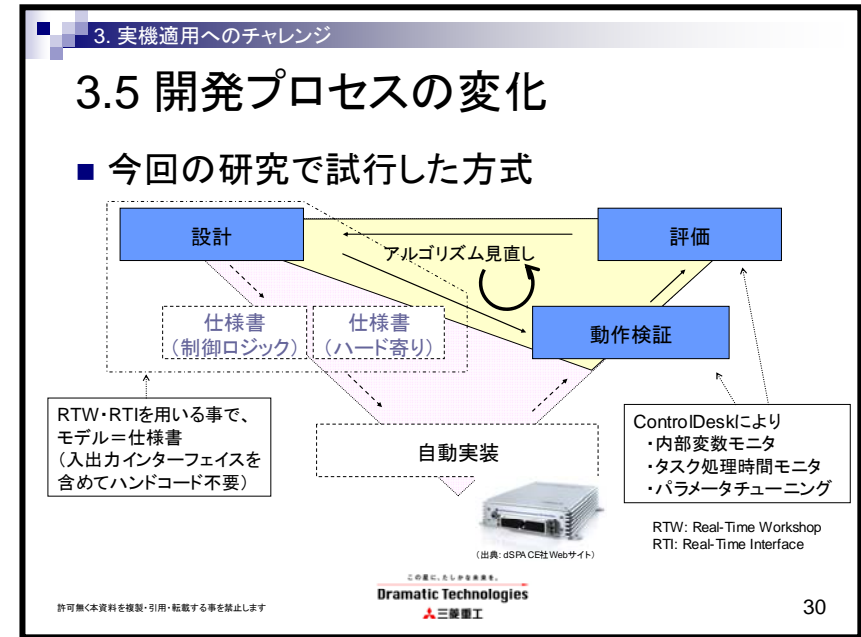
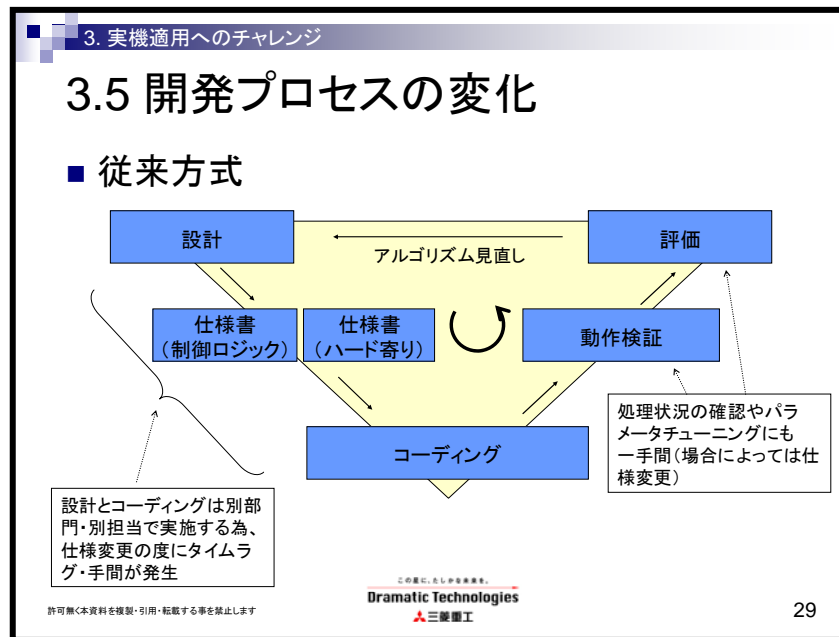
要求獲得ツール
分析・設計支援ツール
数値解析ツール
ソースコード解析ツール
自動コード生成ツール
静的コードチェックツール
コンパイラ/デバッガ
テストツール
検証ツール
評価ボード
インサーキットエミュレータ
アナライザ・測定器
統合開発環境
構成管理ツール
プロジェクト管理ツール
品質管理ツール
ドキュメント管理ツール
その他

0% 20% 40% 60% 80% 100%

出典:2010年版 組込みソフトウェア産業実態調査

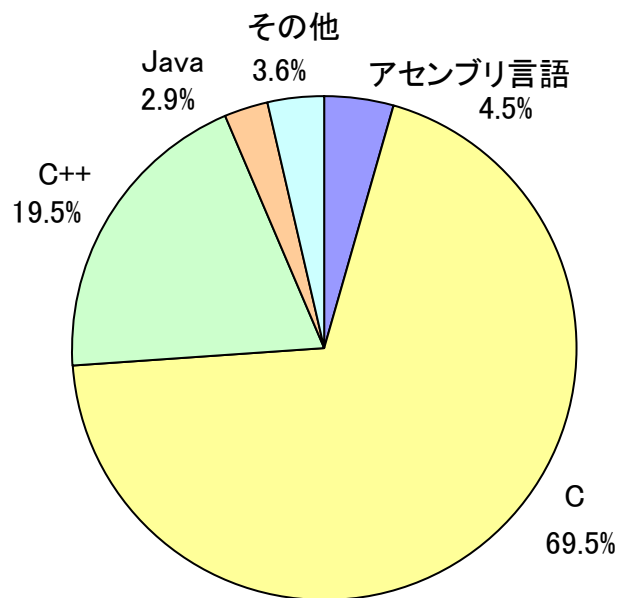
自動コード生成ツールによるソフトウェア実装工程の自動化

- 自動コード生成ツールによるソフトウェア実装工程の自動化が進行
  - 実装工程での品質劣化の防止(開発過程で発生する不具合の約4割)
  - 設計品質の向上(設計工程での「摺り合わせ」が高効率化)
  - 生産性の向上、開発コストの削減、開発期間の短縮
- 自動コード生成が急速に拡大の兆し
  - 止まることのない組込みソフトウェアの大規模化、複雑化 ⇒ 人海戦術が限界に
  - ツール性能、プロセッサ性能、利用技術が向上 ⇒ 自動コード生成が実用レベルに

自動コード生成ツールの採用による開発プロセスの変化(三菱重工業での事例)

三菱重工業株式会社の講演資料より抜粋

使用しているプログラミング言語

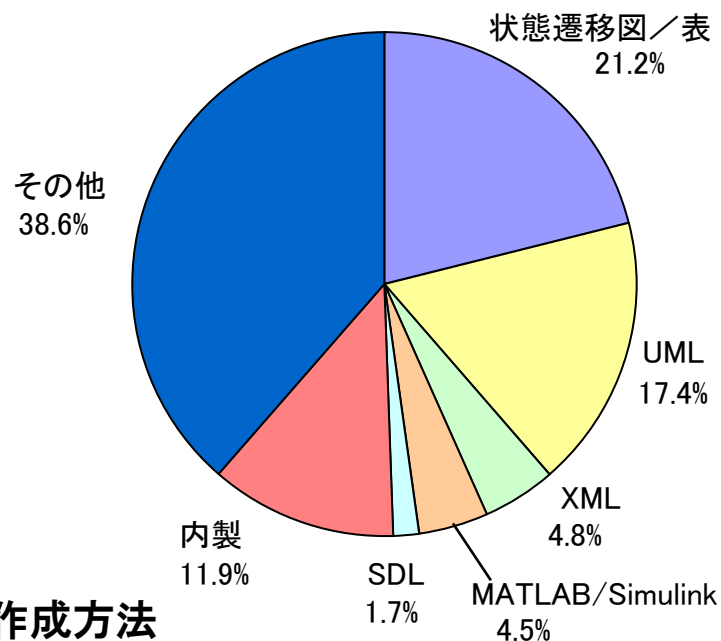
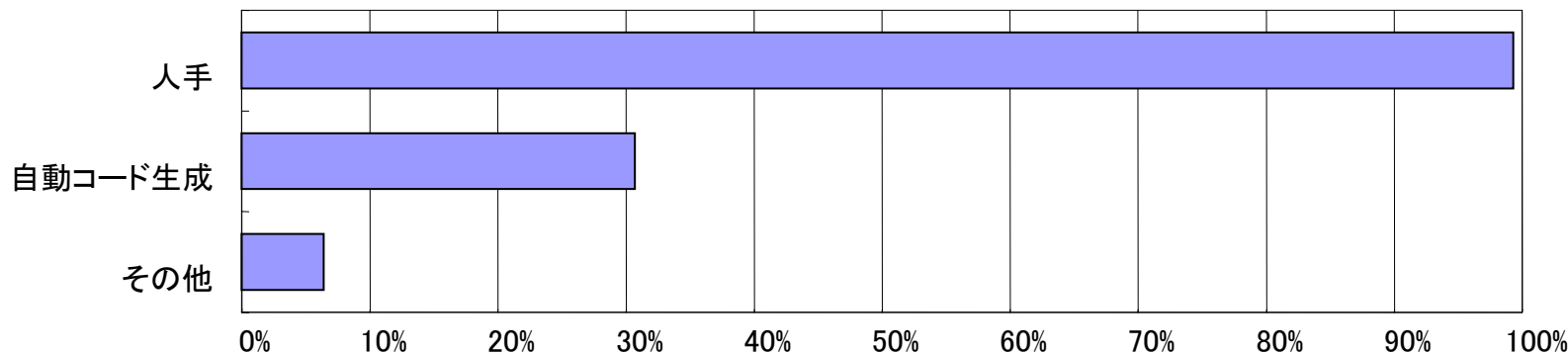
プロジェクト責任者

その他 3.6%
Java 2.9%
アセンブリ言語 4.5%
C++ 19.5%
C 69.5%

使用しているモデルベース言語（自動コード生成）

状態遷移図／表 21.2%
その他 38.6%
UML 17.4%
XML 4.8%
内製 11.9%
SDL 1.7%
MATLAB/Simulink 4.5%

プログラムコード作成方法

人手
自動コード生成
その他

0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%

出典：2010年版　組込みソフトウェア産業実態調査

統合システムに対応する産業界の枠組みを超えた連携強化

- 統合システムとは情報システムと組込システムで構成される大規模システム
- 重要な社会インフラの多くは統合システム
  - 情報システム単体、組込システム単体の信頼性・安全性の確保だけではなく、統合システム全体の信頼性・安全性の確保が重要
- 統合システムの分類
  - 単一型統合システム： 単一目的のために情報システムと組込システムから構成されたシステム
  - 結合型統合システム： 異なる目的で構築された情報システムと組込システムが、それぞれのシステムの利便性を高める目的で結合されたシステム

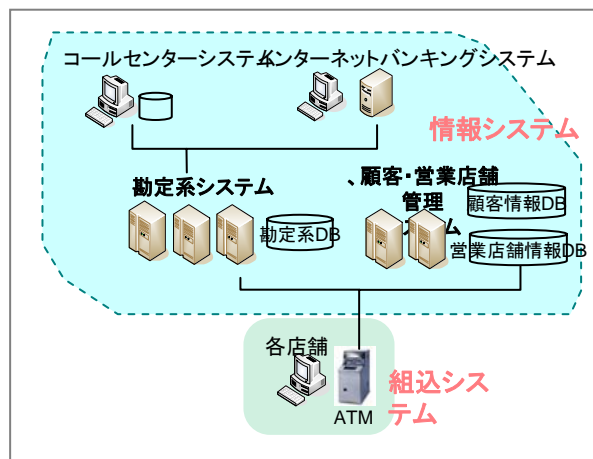
単一型統合システムの例

銀行勘定系オンラインシステム

情報システム：

勘定系システム、顧客・営業店舗管理システムなど

組込システム：

ATM、ネットワークルータ、帳票印刷装置など

結合型統合システムの例

交通管制システムとカーナビゲーションシステム

交通管制システム側の目的：

実車両の位置情報や速度情報により、道路交通状況のより正確な把握ができる

カーナビゲーションシステム側の目的：

交通管制システムの渋滞情報から道路の渋滞状況を考慮した経路案内ができる

統合システム開発の現状と課題

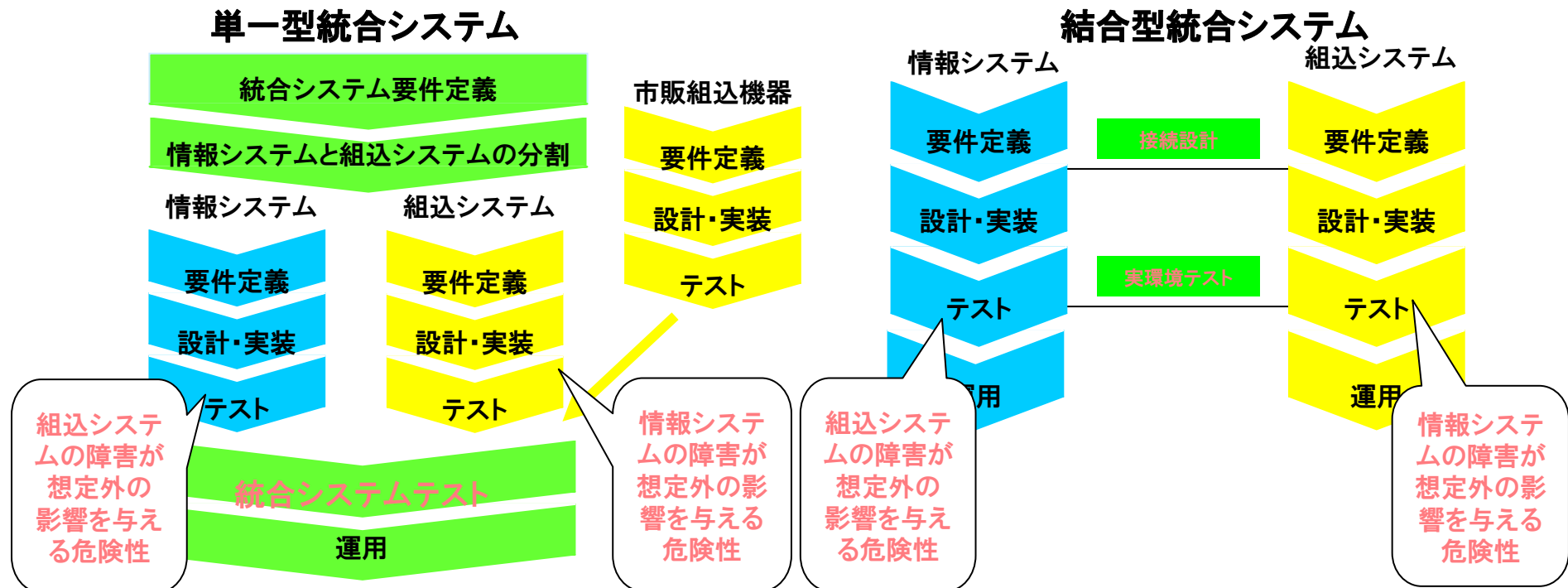
- 統合システムの上流設計段階で、情報システムと組込システムのサブシステムに分割し、サブシステムごとに独立に開発
  - 情報システムと組込システムでは開発者が異なる
  - 統合システム全体としての設計評価が不充分 （統合化は「組合せ」）
- 統合システムの課題
  - 組込システムの障害が情報システムに想定外の影響を与える危険性
  - 情報システムの障害が組込システムに想定外の影響を与える危険性

  ⇒ *障害波及性、システム安定性、サービス継続性の面で潜在リスクが残存*

単一型統合システム

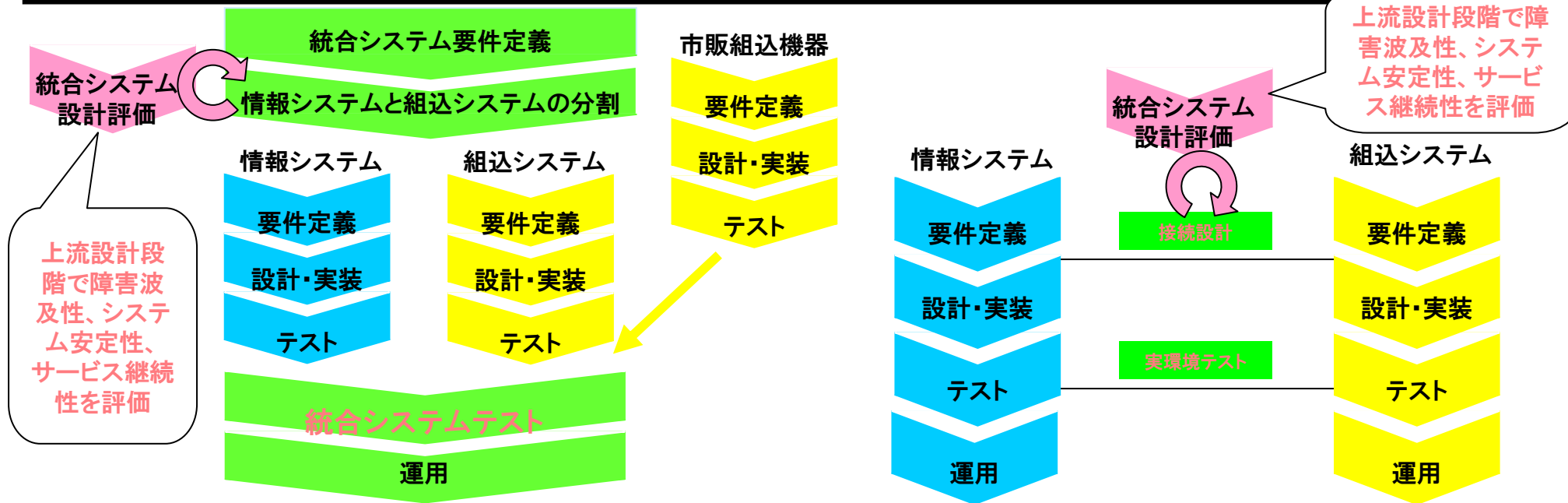
統合システム要件定義
情報システムと組込システムの分割
情報システム
要件定義
設計･実装
テスト
組込システム
要件定義
設計･実装
テスト
市販組込機器
要件定義
設計･実装
テスト
統合システムテスト
運用
組込システムの障害が想定外の影響を与える危険性
情報システムの障害が想定外の影響を与える危険性

結合型統合システム

情報システム
要件定義
設計･実装
テスト
運用
組込システム
要件定義
設計･実装
テスト
運用
接続設計
実環境テスト
組込システムの障害が想定外の影響を与える危険性
情報システムの障害が想定外の影響を与える危険性

統合システムの課題解決へのアプローチ

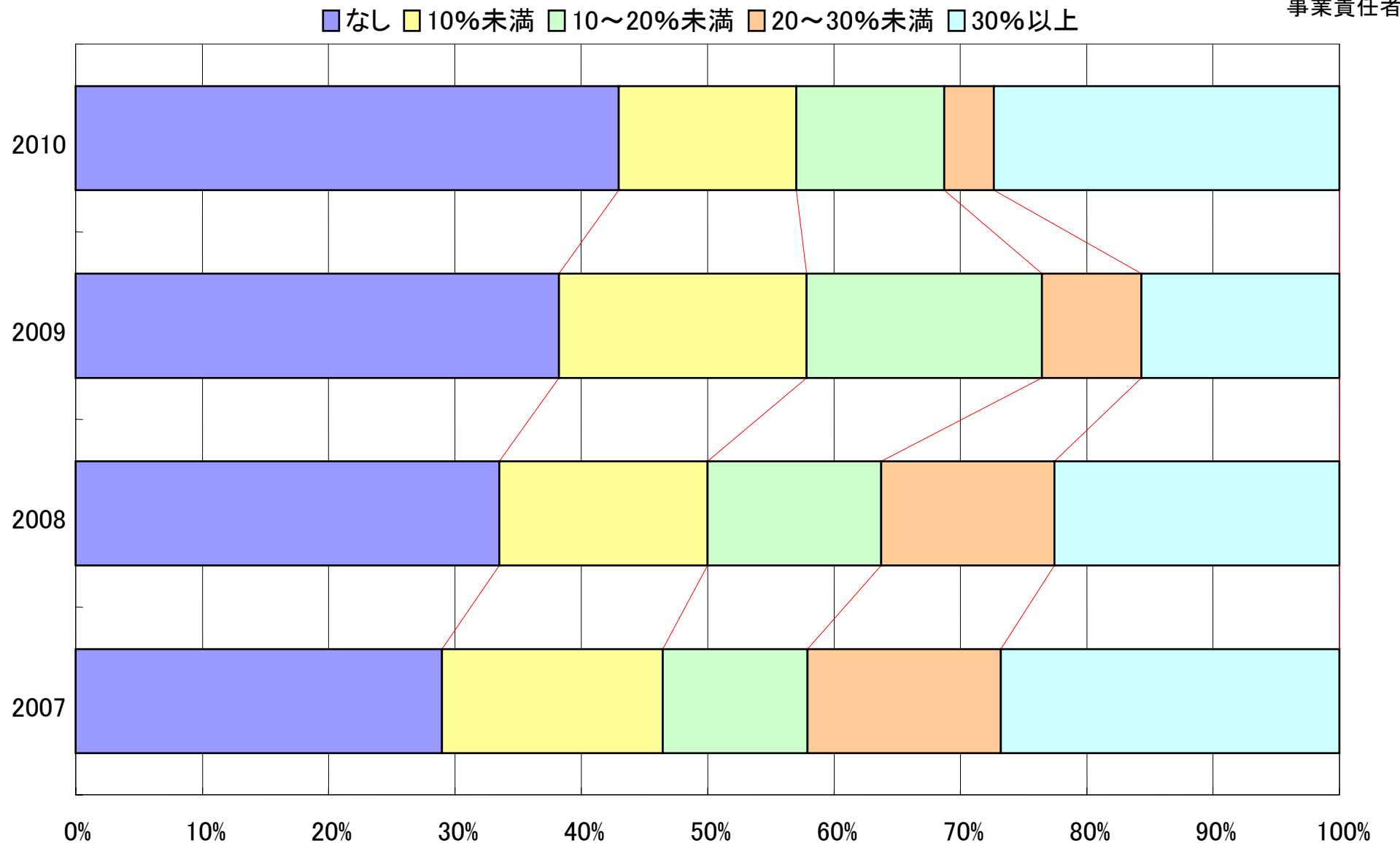
- 統合システムの上流設計段階で、障害波及性、システム安定性、サービス継続性に関する設計評価を実施することにより残存リスクを低減
  - 情報システムと組込システムの共通モデルによる設計評価
  - サブシステムごとのモデルと接続情報から統合システム全体モデルを構築
- 上記のための設計評価環境を整備し、情報システムと組込システムの「摺合せ型」の統合を実現

統合システム要件定義
統合システム設計評価
情報システムと組込システムの分割
市販組込機器
要件定義
設計・実装
テスト
情報システム
要件定義
設計・実装
テスト
組込システム
要件定義
設計・実装
テスト
上流設計段階で障害波及性、システム安定性、サービス継続性を評価
統合システムテスト
運用

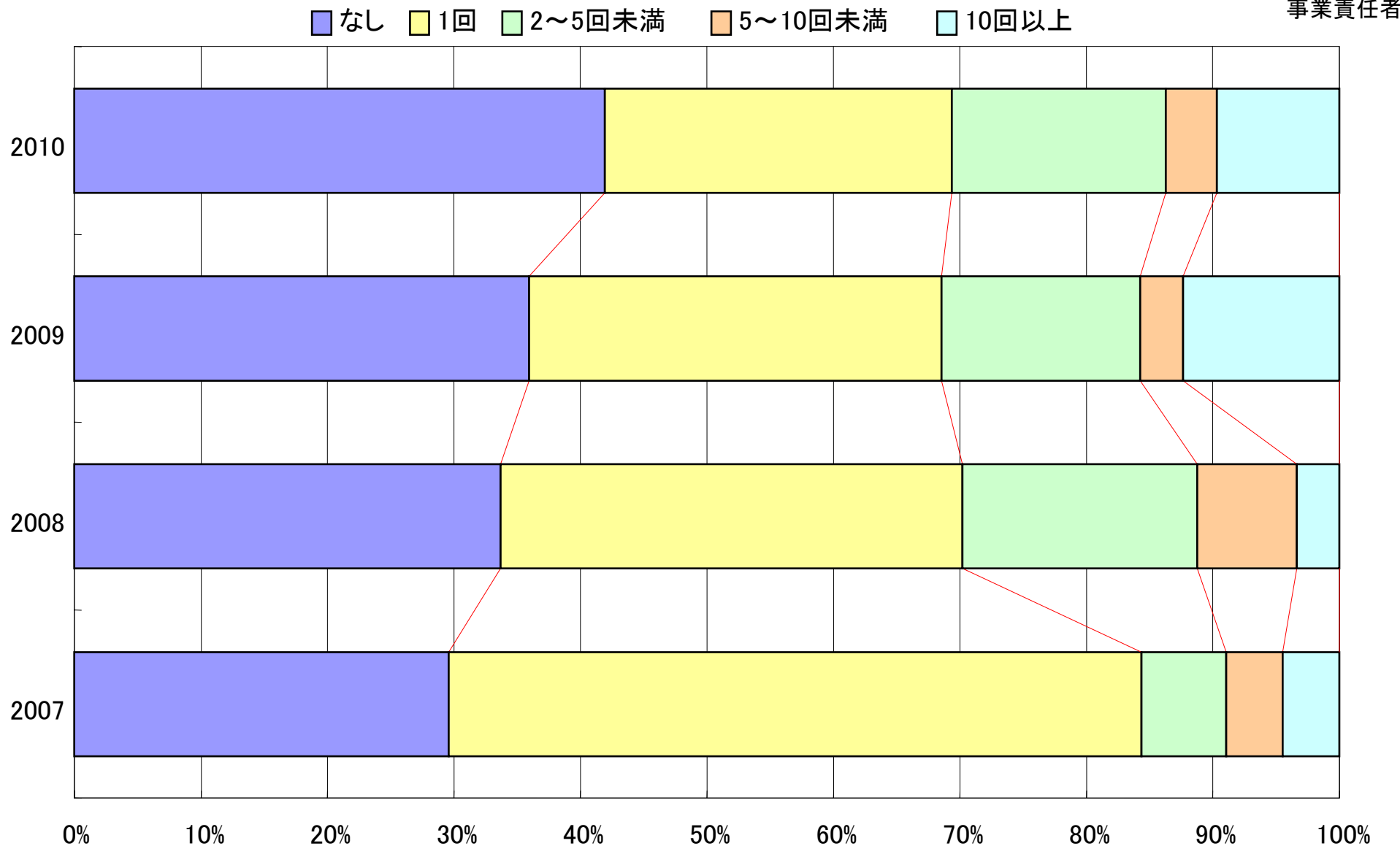
上流設計段階で障害波及性、システム安定性、サービス継続性を評価
統合システム設計評価
情報システム
要件定義
設計・実装
テスト
運用
接続設計
実環境テスト
組込システム
要件定義
設計・実装
テスト
運用

障害波及性、システム安定性、サービス継続性の面で統合システム全体としての潜在リスクを低減

本説明ではサブシステムとして情報システムと組込システムをそれぞれ1つずつ記述していますが、複数の情報システムや複数の組込システムで構成される場合もあります。

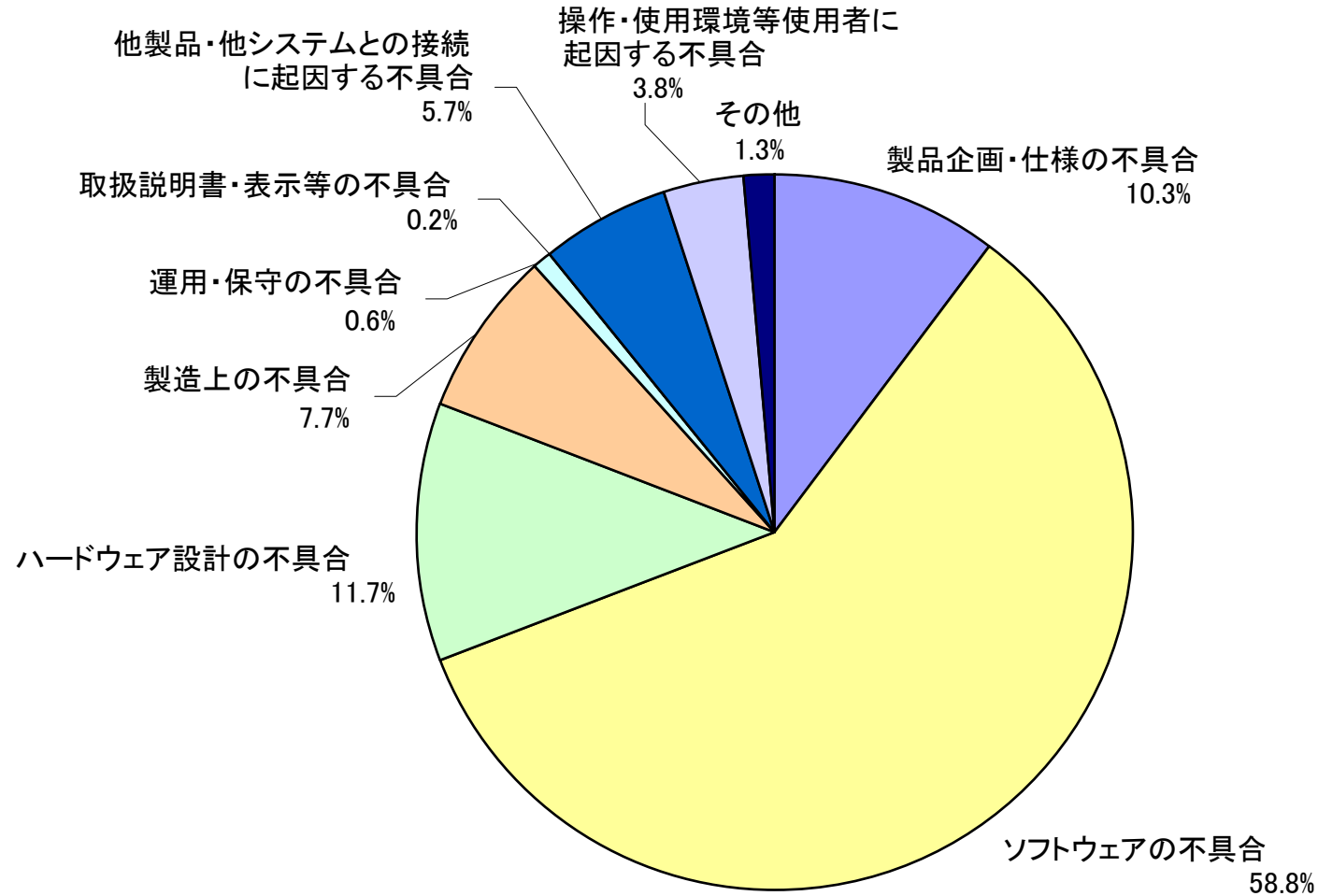
製品出荷後の不具合発生製品率の推移

事業責任者

出典：2010年版　組込みソフトウェア産業実態調査

製品出荷後の1製品あたりの不具合発生回数の推移

事業責任者

出典:2010年版　組込みソフトウェア産業実態調査

不具合の原因の割合(2008会計年度)

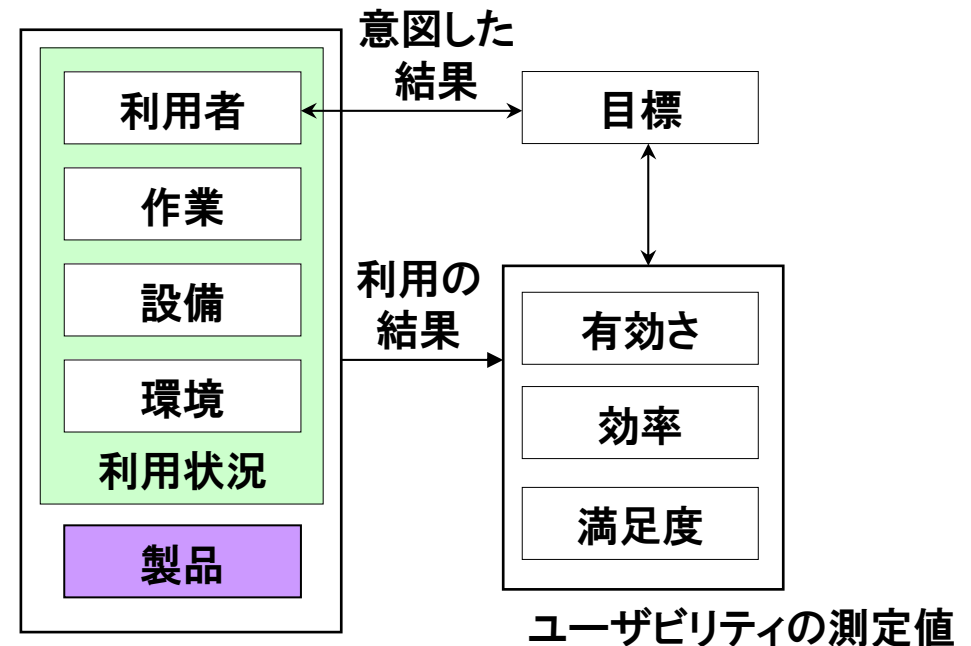
事業責任者

不具合発生件数0を除く

出典:2010年版 組込みソフトウェア産業実態調査

利用品質(ユーザビリティ)の定義

ISO 9241-11: Guidance on usability （JIS Z8521）

指定された利用者によって、指定された利用状況の下で、指定された目的を
利用者が
有効に、効率良く、満足して
達成できるための製品の能力

ISO 9126(ソフトウェア品質)における
利用品質とほぼ同じ定義となっている。

平沢尚毅氏　ESEC2005専門セミナー資料

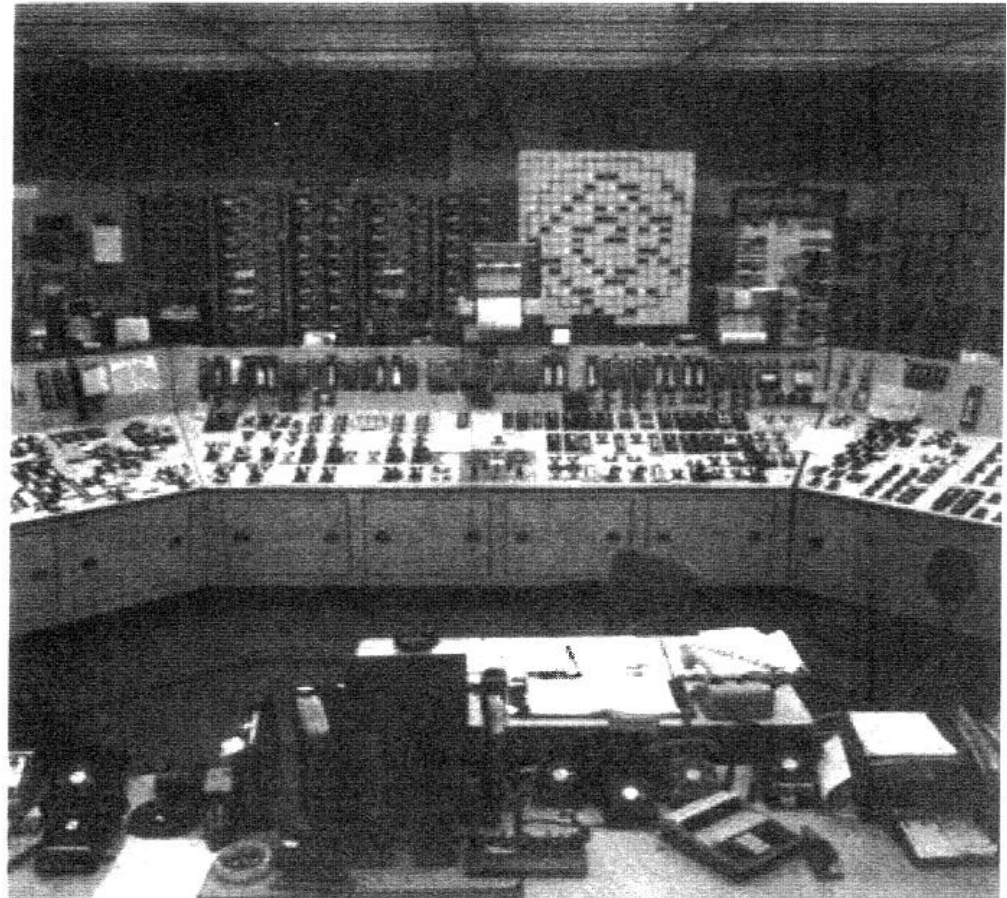
·有効さ (Effectiveness): ユーザが指定された目標を達成する上での正確さ、完全さ
·効率 (Efficiency)　　: ユーザが目標を達成する際に正確さと完全性に費やした資源
·満足度 (Satisfaction) : 製品を使用する際の、不快感のなさ、及び肯定的な態度
·利用状況 (Context of use): 製品が使用される物理的及び社会的環境。

ユーザビリティの始まり

スリーマイル島原発事故(1979. 3.28.ペンシルバニア)

この事故から認知的な研究、体系化がスタート

・機器の故障+運転員のヒューマン・エラー

- 人間工学
- 認知科学
- 信頼性工学
- 行動科学
- 働態学
- 知覚心理学
- 行動心理学
- 産業心理学
- 言語学、など

The control room at the Three Mile Island nuclear power plant .[5]

受容性に着目した分類

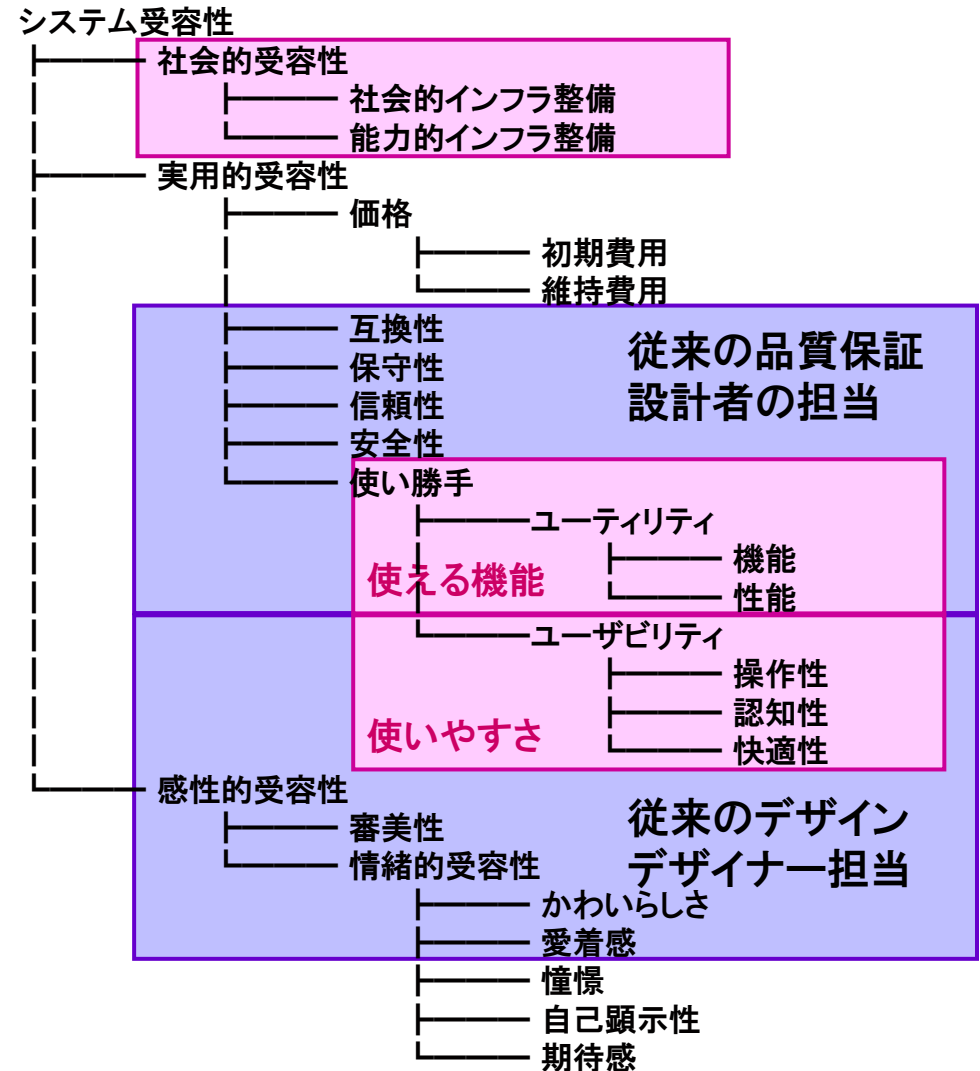
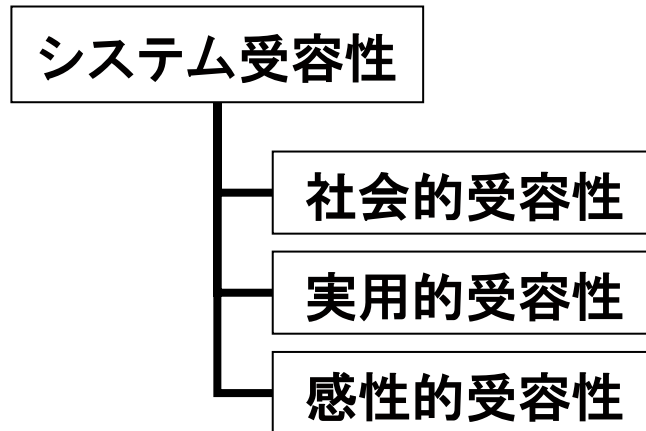
ユーザ(消費者)が
受け容れる事柄を分類
(Nielsen+ Kurosu)

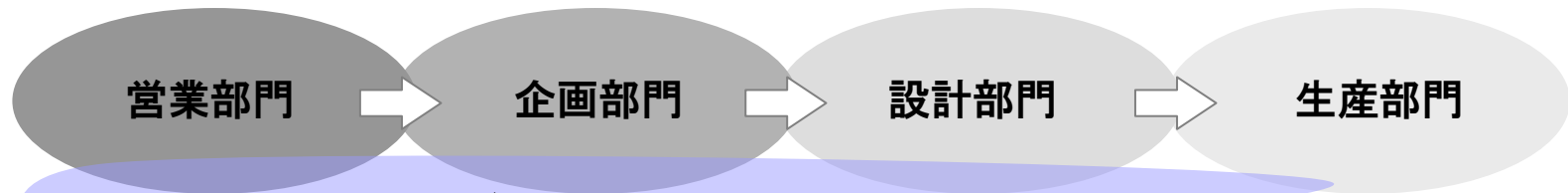
システム受容性
- 社会的受容性
  - 社会的インフラ整備
  - 能力的インフラ整備
- 実用的受容性
  - 価格
    - 初期費用
    - 維持費用
  - 互換性
  - 保守性
  - 信頼性
  - 安全性
  - 使い勝手
    - ユーティリティ
      - 機能
      - 性能
    - ユーザビリティ
      - 操作性
      - 認知性
      - 快適性
- 感性的受容性
  - 審美性
  - 情緒的受容性
    - かわいらしさ
    - 愛着感
    - 憧憬
    - 自己顕示性
    - 期待感

従来の品質保証
設計者の担当

使える機能

使いやすさ

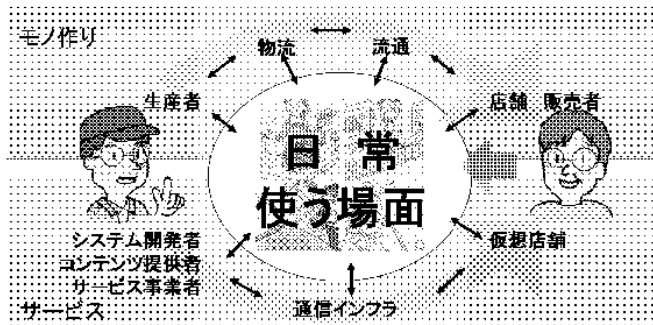
従来のデザイン
デザイナー担当

ユーザ情報の扱い

ユーザ情報を開発プロセスの各工程で有効に活用していく仕組みが必要

ユーザ情報を営業･企画･設計･生産の各工程で活用する

ユーザビリティの開発意識

常にエンドユーザの利益を意識し、配慮する

従来の開発要素に「使う場面」を追加して考える

＋

機能安全＋ユーザビリティの開発意識

常にエンドユーザの利益を意識し、配慮する

従来の開発要素に「想定外に使う場面」を追加して考える

形式手法適用(実用化)海外事例

形式手法が進む欧州においては、いまだ限定的だが重要インフラを中心に適用(実用化)が進んでいる（情報系よりも組込み系が主、企業情報システムでは、セキュリティやネットワーク関連が中心）

形式手法の情報システム系重要インフラへの適用 (実用化) の概要

重要インフラ領域	適用国	システム名	適用企業･機関（システムベンダーなど）	適用開発工程	適用形式手法･ツール
情報通信	独	ネットワークプロトコル仕様	Lucent Technologies Network Systems GmbH	設計	ADeVA(言語入力、VHDL変換)、GateProp（モデル検査)、VHDL
	伊	船舶向け通信システム	Selex Communications、University of L'Aquila	設計･テスト	CHARMY(アーキテクチャ･時相制約記述、SPINへの変換)、DEPCOL(性質抽出)
金融	インド	生命保険関連情報システム	The Research Development and Design Centre	要求分析	Requirements Modeling Tool (図からSAL形式への変換･解析)
航空	英	航空機エンジン制御システム	University of York	設計	SCANN、SLANN(独自の設計手法)、HAZOP(リスク分析手法)
鉄道	仏	鉄道制御システム、駅乗車ホーム防御ドア制御システム	ClearSy、Siemens Transportation Systems	設計、実装	B、Atelier B、EDith B、Bertille(仕様詳細化支援ツール)、Brama、LADDER(言語)
電力･ガス･水道	独･韓国	原子力発電所制御システム	Institut fuer Sicherheitstechnologie、Korea Atomic Energy Research Institute	設計	N/A
政府･行政･医療ほかその他 注)組込み系を一部含む	独	セキュリティ(医療情報システムアクセス制御、スマートカード等)	Siemens Corporate Technology	設計	Isabelle(定理証明)、モデル検査(独自)、Interacting State machines(独自のオートマトンモデル)
	仏	マイクロカーネル(L4OS)	STMicroelectronics、ClearSy	テスト	Event B、Brama

出所：「高信頼性ソフトウエア構築技術に関する動向調査」（2008年10月、独立行政法人情報処理推進機構、情報源は05年以降の国際会議等に発表されている論文や報告書等の文献）ほか

欧州事例：オランダ防潮可動橋管理システム

事例概要

- オランダ運河のマエスラント防潮可動橋（水門）（Maeslantkering）
  - Rijkswaterstaat(State Department for the Maintenance of Ways and Waterworks 国家水路・水事業保全省)管轄Deltaworksプロジェクトの一環
  - 暴風等による運河水位上昇・洪水防御のゲート（径360m）
  - 98年竣工し、97年以来毎年開閉のテストを行うも、06年に同システム信頼性を懸念、アップグレードに際し、客観的評価実施、形式手法を用いる
  - 稼働に影響を及ぼすソフトウェア上の欠陥は発見されず
  - 07年11月11日、実際の暴風雨に対し初めて水門を閉鎖

マエスラント防潮可動橋（水門）の全容

運河上空写真（水門開放時）

出所：FM2008（第15回形式手法国際シンポジウム・インダストリーデイ公式サイト　http://www.fm2008.abo.fi/industry_day　、ガートナーコンサルティング取りまとめ

欧州事例：英国航空管制システム(iFACTSプロジェクト)

iFACTS(interim Future Area Control Tools Support)は形式手法適用の英国最大プロジェクト。

iFACTSプロジェクト概要

- ユーザー： NATS(National Air Traffic Services)
- 場所： Hampshire Swanwickロンドン地区管制センター
- 背景：
  - 英国政府では、旅客者数が2020年までに現在の2倍、30年までに同3倍へ急増すると試算
  - 2013年までに年間フライト数3百万本へ対応(現2.3百万本)
  - 新技術を採用した管制システムの導入、管制官への旅客機航行支援、安全性の確保が不可欠と判断
- プロジェクト費用：
  - 総費用50百万ポンド(約70億円、1ポンド=140円換算)
  - Praxis受注額10百万ポンド(同、約14億円)
- システム概要：
  - レーダーシステム有史来最大・革命的な航空管制(ATC)システム
  - 航空管制システムとしては、世界で最先端
  - 航空機が航行計画に従わず航路を外れた場合、管制官に対し事前に警告を発し、衝突回避等のための判断情報を提供する
  - 完全な電子データによる管理、洗練された複数ディスプレイ・モニター
- 形式手法ベンダ：Praxis
  - 仕様記述、ATSシステムソフトウェアの開発
  - Correctness by Construction、SPARKの適用
- 他ベンダー：
  - Lockheed Martin
  - IBM
  - AdaCore、など

Swanwickロンドン地区管制センターの様子

出所：Praxis07年3月7日プレスリリース、"Correctness by Construction of High Integrity Software"(07年、Rod Chapman, Praxis)、BBCニューズ記事(07年3月7日)他、ガートナーコンサルティング取りまとめ

欧州事例：フランス地下鉄乗車ホーム防御ドアシステム

乗車ホーム防御ドア
（COPPILOT：地下鉄13号線）

システム概要（SIL4）
（Dof1：地下鉄1号線）

Tail On-Board DOF1
Train normal way
Head On-Board DOF1
S2
S1
Tail On-Board DOF1 sensor (train bogie)
Platform Tail DOF1 mat (on the rails)
Platform DOF1
"Train automation" system
"Platform Doors" system
platform technical office（乗車ホーム管制室）
Platform Head DOF1 mat (on the rails)
Head On-Board DOF1 (train bogie)

sensor
（各種センサー）

On board DOF1
（列車組込み系）

Automaton
（セキュリティ・オートメーション・システム）

mat

PSDは列車組込みソフトと外部システム（各種センサー含む）との組合せ

出所：ClearSy現地インタビュー、“Formal Methods in Safety-Critical Railway Systems”（ClearSy）、“Provides safety critical systems and software”（ClearSy）、
FM2008 (第15回形式手法国際シンポジウム・インダストリーデイ公式サイト
http://www.fm2008.abo.fi/industry_day、ほか

IV&V(独立検証&妥当性確認)の事例:パリ交通局の鉄道システム

- RATP(パリ交通局)におけるサプライヤと協調して行われる 開発/妥当性検討/安全分析 のプロセス。
- 設計、製造、テスト、検証のV字開発プロセスにおいてRATPとサプライヤが協調しながら、安全システムの設計を進める。RATP発注部門・サプライヤ部門の第三者としてRATP安全チームが安全系の開発を検証。

システム一般設計

試運転

操作要求
エンドユーザ仕様

安全計画
暫定危険分析

使用試験

論理
セーフティケース

システム詳細設計

システム妥当性検証と統合

システム仕様
機能インタフェース仕様
機能機器仕様

システムFMEA
インタフェース危険分析
機器FMEA(注1)

危険ログ
安全プロセス評価
安全分析

システム機能テスト
システム統合テスト

セーフティケース (注2)

危険ログ
安全評価

コンポーネント製造

機器妥当性検証

HW/SW仕様
一般使用書類
詳細仕様書類
生産/コーディング

SW安全分析
HW安全分析

安全SW評価
安全HW評価

妥当性検討テスト
統合テスト
単体テスト

SW安全分析
HW安全分析

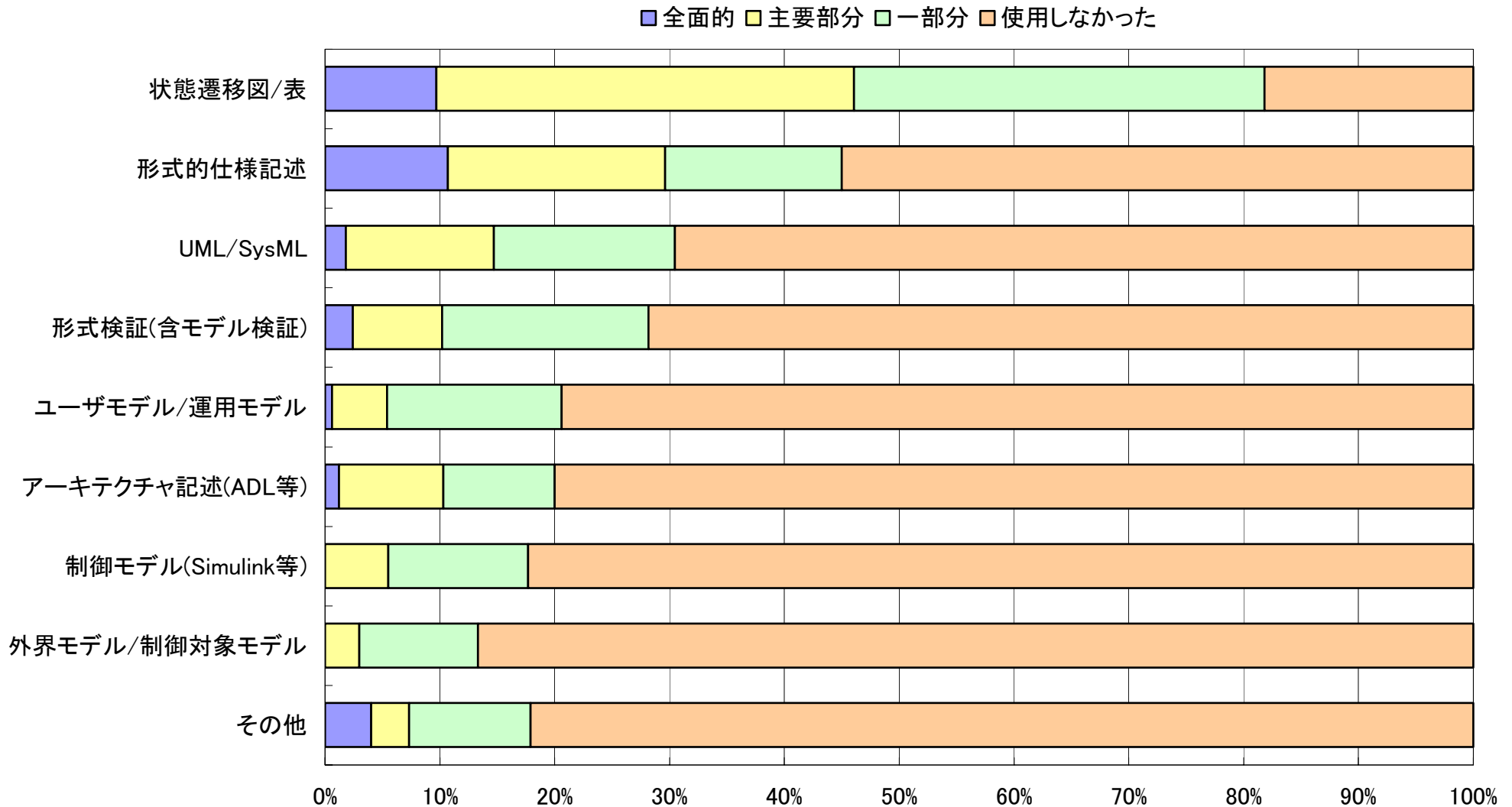
補完テスト
安全評価

RATP | RATP安全チーム | サプライヤ | サプライヤ安全チーム

RATPプレゼンテーション資料よりガートナー作成

注1:Failure Mode and Effect Analysis(故障モードとその影響の解析)は、故障・不具合の防止を目的とした、潜在的な故障・不具合の体系的な分析方法
注2:システムの安全を示す書類で、安全性を示す証拠書類(Evidence)と安全性の論拠を示す論拠(Argument)からなる。

プロジェクトで利用した手法・技法

プロジェクト責任者

出典:2010年版 組込みソフトウェア産業実態調査

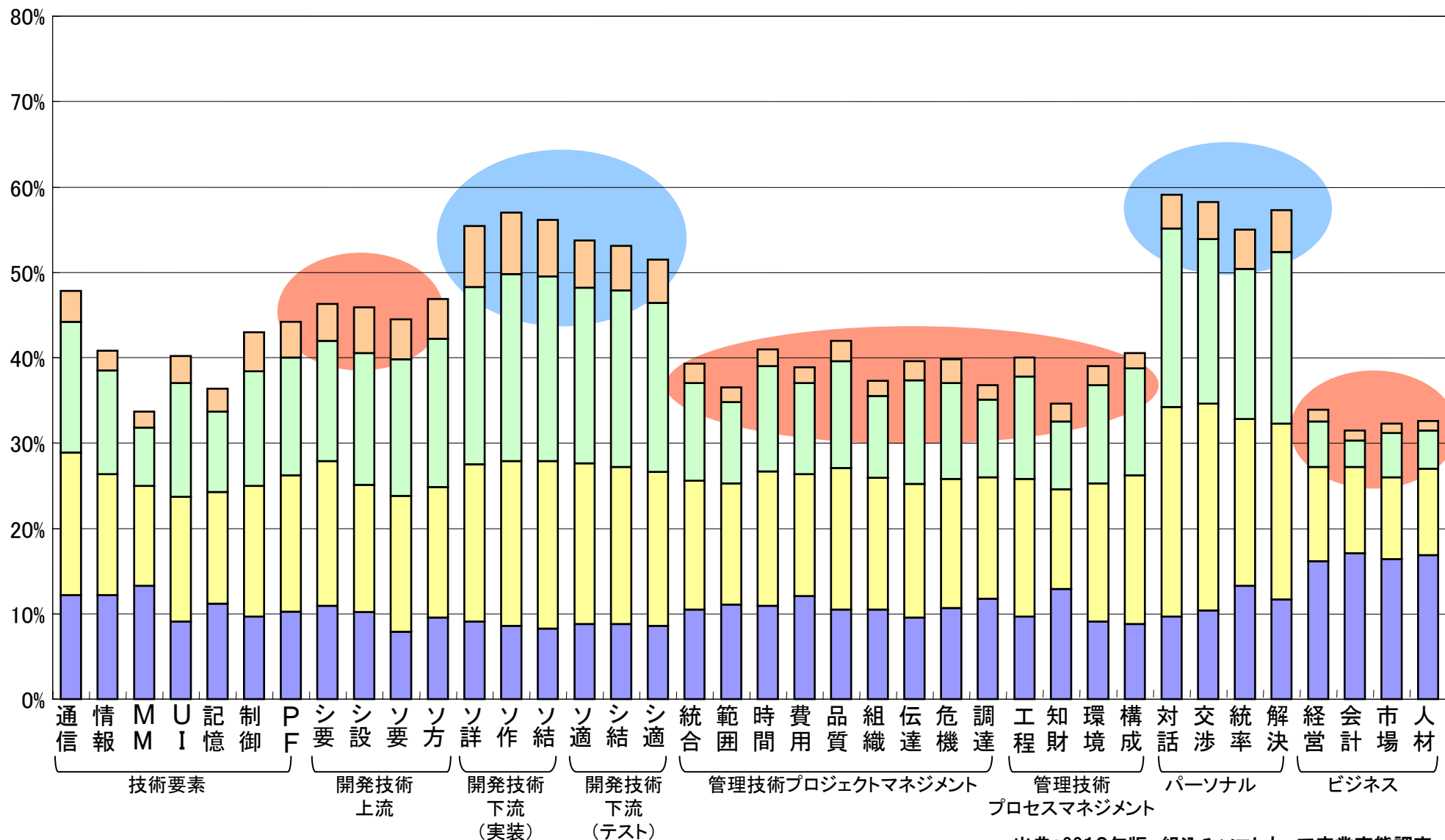
プロジェクトの平均的スキルプロファイル(社内＋社外)

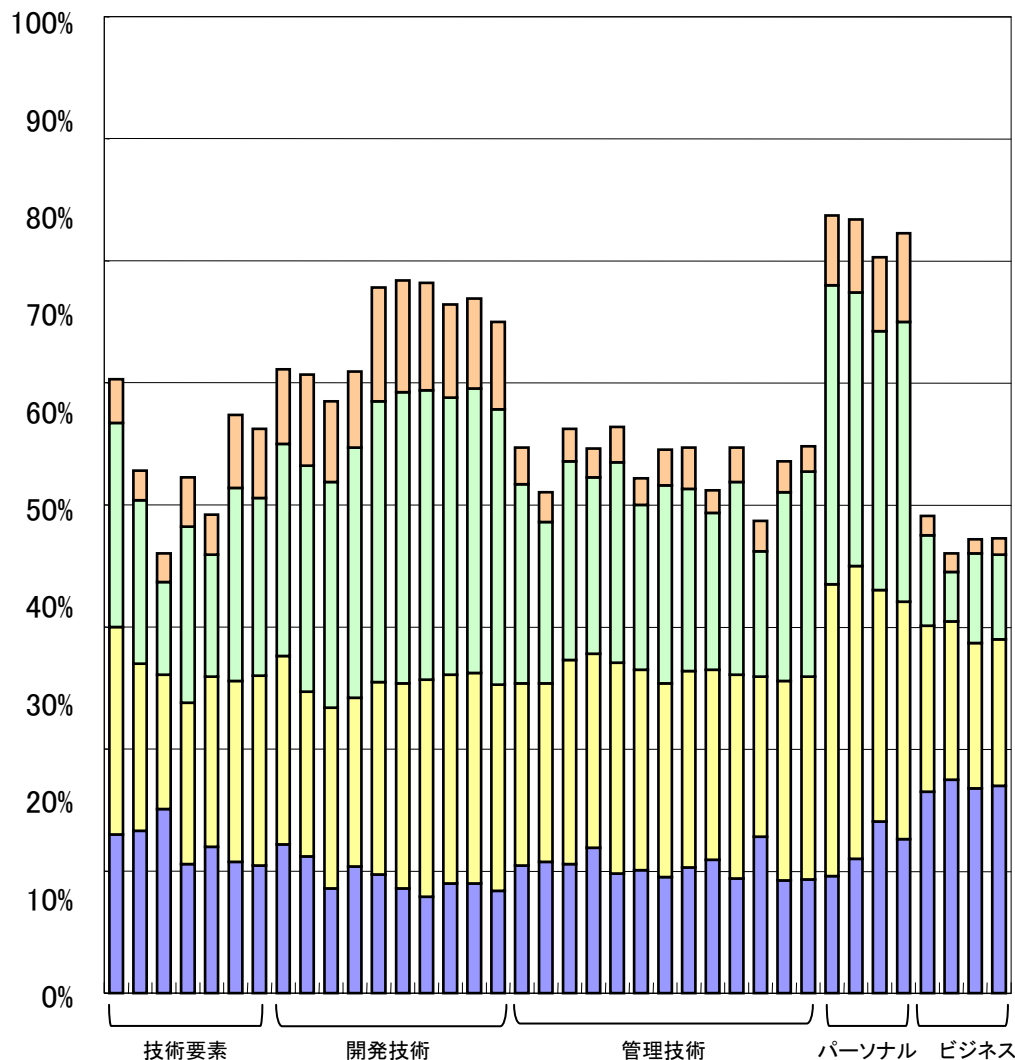
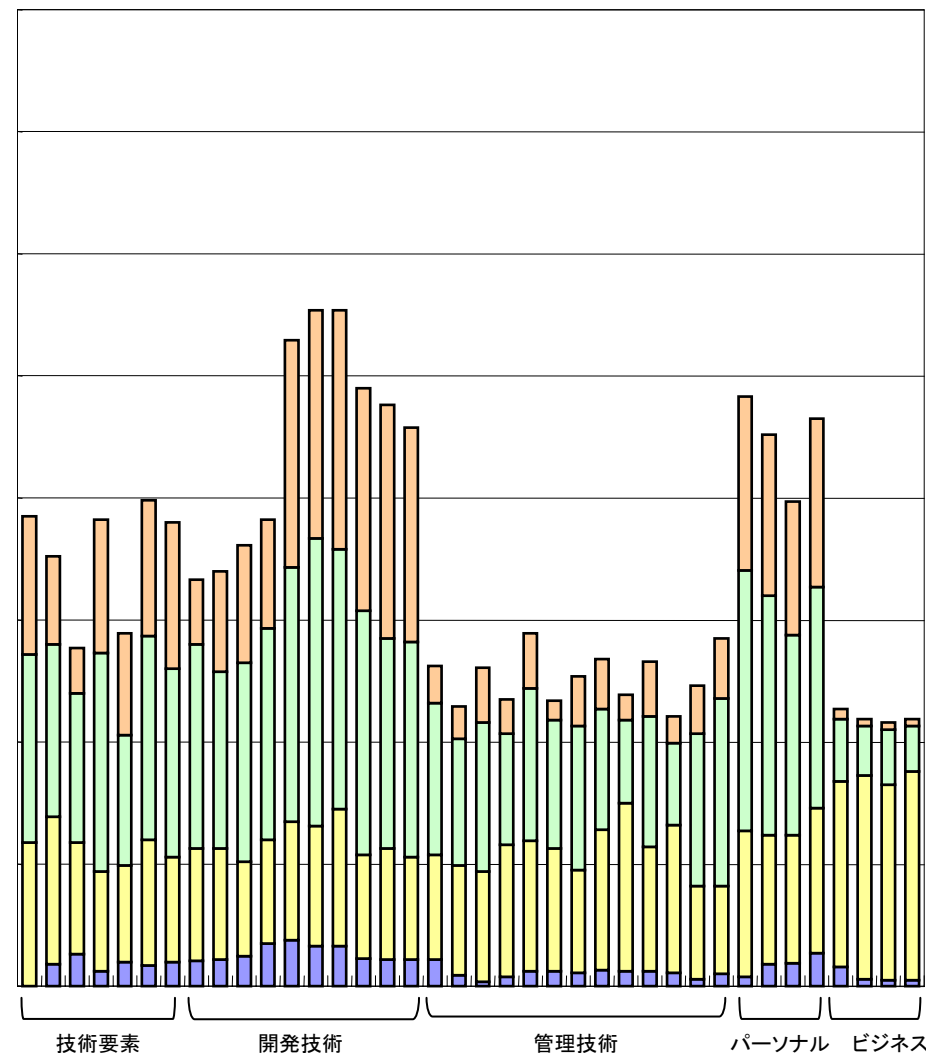
レベル1　レベル2　レベル3　レベル4

プロジェクト責任者

80%
70%
60%
50%
40%
30%
20%
10%
0%

通信　情報　MM　UI　記憶　制御　PF　シ要　シ設　ソ要　ソ方　ソ詳　ソ作　ソ結　ソ適　シ結　シ適　統合　範囲　時間　費用　品質　組織　伝達　危機　調達　工程　知財　環境　構成　対話　交渉　統率　解決　経営　会計　市場　人材

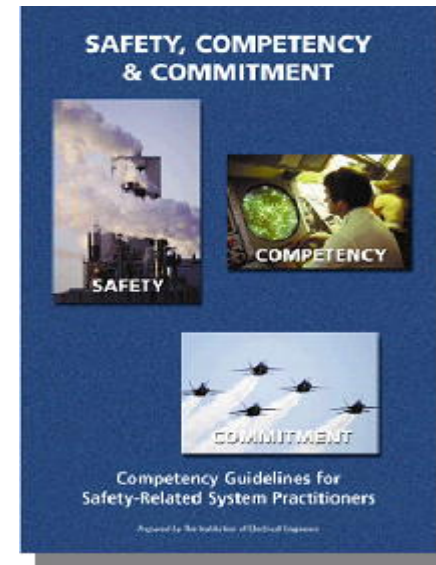
技術要素　開発技術 上流　開発技術 下流 (実装)　開発技術 下流 (テスト)　管理技術プロジェクトマネジメント　管理技術 プロセスマネジメント　パーソナル　ビジネス

出典:2010年版　組込みソフトウェア産業実態調査

社内と社外のスキル評価の比較

プロジェクト責任者

出典:2010年版 組込みソフトウェア産業実態調査

安全系従事者のコンピテンシ指針

。安全関連系従事者には、担当業務にふさわしいコンピテンシ（資質・行動特性）が求められる。英国ではHSE（健康安全庁）の指導の下で、1999年に「コンピテンシ指針」が出版され、英国における機能安全認証で引用されている。

「コンピテンシ指針」英国ではHSE（健康安全庁）の指導の下で、1999年に出版

英国における機能安全認証に引用

更に、2007年、この指針を実施するための手引き「**安全関連系のためのコンピテンシ管理**」が公開された。

（右記サイトから無償入手可能：http://www.hse.gov.uk/consult/condocs/competence.htm）

この中で、コンピテンシ管理の進め方のほか、担当者の選定と採用、アセッサーと管理者のコンピテンシの管理、外部供給業者のコンピテンシ管理までが規定されている。

consulting

安全系従事者のコンピテンシ指針(HSE;英国健康安全庁):構成

HSEのコンピテンシ指針は、①コンピテンシとして技術的コンピテンシと人間行動のコンピテンシが定義される。また、②組織が持つべき機能が定義される。各機能で、必要なコンピテンシに対応する機能番号(例えばCFM10)が定義され、各機能番号に対応する③コンピテンシのレベルが評価される。

② 機能(組織が持つべき機能) - - - - -> ETSSの職種に相当

① コンピテンシ - - -> ETSSのスキルに相当

コンピテンシ		CFM	PSM	SRM	SRP	ISA	HRA	SRS	SV	SAD	SHR	SSR	HF
技術的コンピテンシ	責任の割り付け						HRA8	SRS4	SV7	SAD4	SHR8	SSR9	
	試験結果の分析								SV10				
	コードの解析				SRP7								
	設計の分析							SRS6					
	ハードウェア設計の分析							SRS7					
	安全分析の審査		PSM11										
	見積提案書の審査	CFM10	PSM7	SRM11	SRP8	ISA12							HF7
	審査戦略の選択		PSM6										
	スタッフコンピテンシーの保証	CFM11				ISA11							
	合計69												
人間行動のコンピテンシ	応用領域に関する知識	CFM2											
	正確さと細部への配慮								SV4				
	事業の目的											SSR5	
	明確さ											SSR3	
	概念思考と寛大さ					ISA6					SHR4		
	意思決定				SRP3								
	効果的伝達					ISA2							
	作業の場における効果的相互関係	CFM9											
	合計29												

③ コンピテンシレベル - - - -> ETSSのスキルレベルに相当

- 専門家
- 実務者
- 監督を受ける実務者

安全系従事者のコンピテンシ指針(HSE；英国健康安全庁)：コンピテンシ評価基準の例

技術コンピテンシの例

SSR4　コーディング		
規定されたソフトウェア機能および設計要求事項を，適当なプログラム言語を正しく使用することを通して，容易に理解でき分析可能なソースコードに翻訳する。関連するコーディング規格に当然の注意を払う。		
監督を受ける実務者	実務者	専門家
組織のプログラミングスタイルとコメント戦略に従った関連するプログラム言語を用いて個々のモジュールのコード化を行った。	定義されたコーディング規約に従った，関連するプログラム言語の安全サブセットを用いて典型的安全関連系のための完全なソフトウェア部分のコード化を行った。	ソフトウェア工学研究，特に不安全な構成と避けなければならない状況に関する最近の開発に遅れずついて行っている。また体系的コーディング規約についての最新の理解を維持している。

人縁行動コンピテンシの例

ISA15　専門職としての立場と個人的強さ		
信頼できる判定を下せる専門職としての立場にいる，すなわち，権威者として広く認められ，外部圧力がかかっても信念を変えない強さをもつ人物であること。		
監督を受ける実務者	実務者	専門家
判定に際し，妥協することを強いられたとき，強い信念が重要であることを認識している。	地位を危うくするような外部圧力がかかっても判定を変えなかった。	安全に関しては、外部干渉により妥協を強いられるような状況でも判断を変えないことにより，職務への信念が強いとの評判を得ている。

セーフティケース

鉄道のような安全の重要性が高く、事故が起こった場合に社会への影響が大きい産業で採用されている。英国では原子力分野へも展開しており、自動車規格ISO26262においても採用されている。

セーフティケースの定義 (IAEA安全用語集)：

「ある施設又は活動の安全を裏付ける議論と証拠を収集したもの」

通常、安全評価の結果及びこれらの結果の信頼性の証明からなる。

例：

①EUROCONTROL(欧州航空航法安全機構)

EUR RVSM (短縮垂直間隔;Reduced Vertical Separation Minimum)導入のためのセーフティケース

②EUROCONTROL(欧州航空航法安全機構)

EUR 全空域ATMシステムのセーフティケース

③DTI(英国貿易産業省)

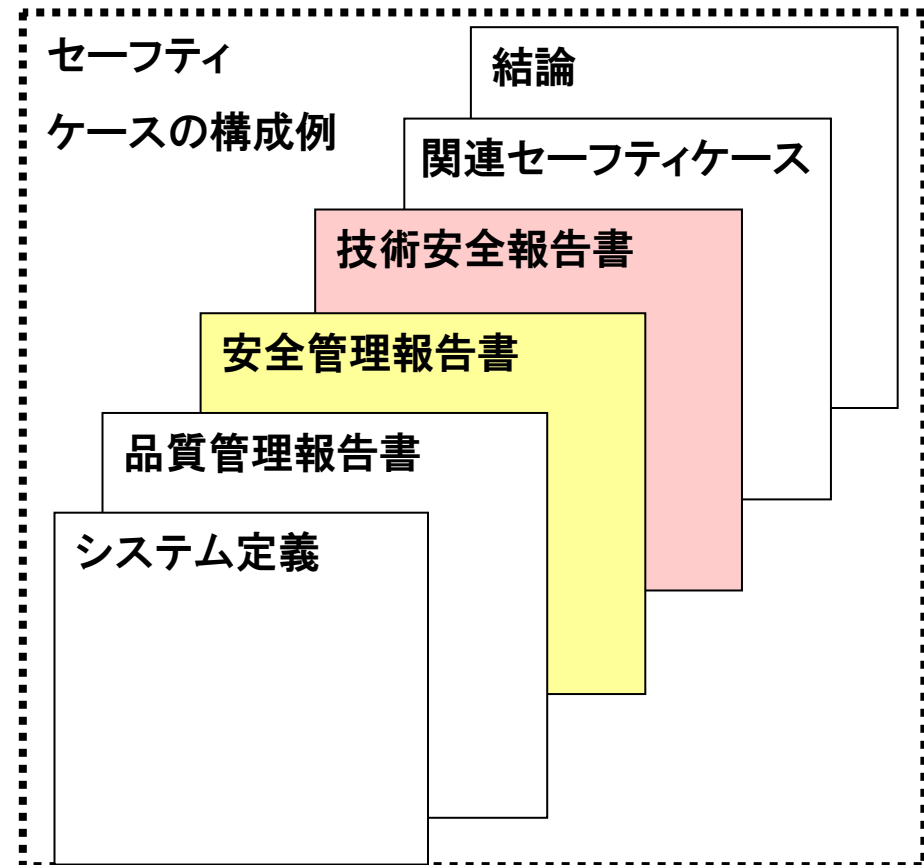
電力配電回路網における電流制限装置使用のためのセーフティケース

④スイスNAGRA(放射性廃棄物管理共同組合)

Opalinus Clay 処分場セーフティケース

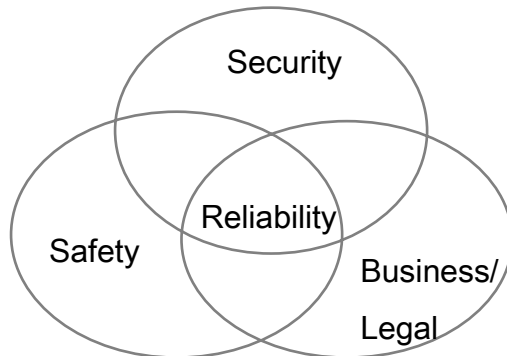
⑤LU(ロンドン交通局・地下鉄)

ロンドンの地下鉄の契約セーフティケース

アシュアランスケース

セーフティケース

ある環境のあるアプリケーションにおいて、システムの安全の的確性の議論と裏付けとなる証拠の書類

A documented body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment

ASCAD—Adelard Safety Case Development Manual

- **他のドメイン（例：セキュリティ）への拡張**
- **統一化された構造による記述**
- **標準化を意識**
- **他の標準との協調**

アシュアランスケース

ある環境のあるアプリケーションにおいて、システムの属性に関する一連の主張を正当化する議論と裏づけとなる証拠

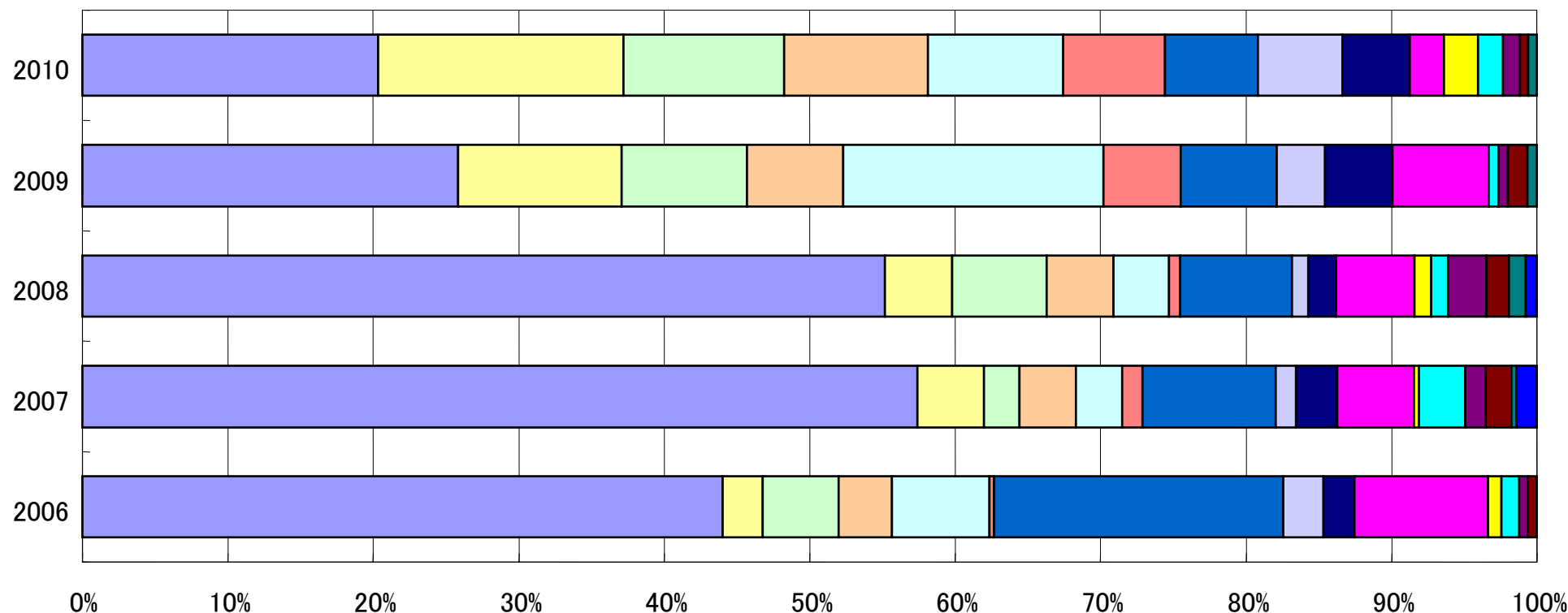
A documented body of evidence that provides a convincing and valid argument that a specified set of critical claims about a system's properties are adequately justified for a given application in a given environment.

重要と考える政府施策

経営者

- 組込みソフトウェアの開発を狙う人材の育成
- ものづくり基盤技術分野の戦略に基づく中小企業への支援策の強化
- 高付加価値部材・技術の叢生に向けた、高リスク研究開発の支援
- 基盤的な要素技術や共通基盤的技術の開発
- 国際的なビジネス展開・市場拡大のための環境整備
- 経営資源の潜在力を引き出すIT活用推進
- 安全性の確保、PL法上の取扱い、各種保険制度等の制度整備
- 国際的な連携強化による、海外リソースの活用
- 人材・研究開発・IT投資等の促進税制
- 標準化課題の整理と国際標準化の主導権の確保
- ルール整備、情報開示、政府調達などによる市場の創出・拡大
- ものづくり分野・戦略分野における専門職大学院の設置
- 職種別スキル標準の整備等による、人材育成の強化
- 川上企業・川下企業間のネットワーク構築支援
- 知的資産の評価・管理・活用・開示のための手法作り
- 地域独自の戦略に基づく地域基礎力の強化

2010
2009
2008
2007
2006

0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%

出典:2010年版 組込みソフトウェア産業実態調査

重要と考える政府施策と地域施策

■政府の施策 □地域の施策

事業責任者

組込みソフトウェアの開発を担う人材の育成
人材・研究開発・IT投資等の促進税制
ものづくり基盤技術分野の戦略に基づく中小企業支援策の強化
標準化課題の整理と国際標準化の主導権の確保
高付加価値部材・技術の創生に向けた、高リスク研究開発の支援
ルール整備、情報開示、政府調達等による市場の創出・拡大
基盤的な要素技術や共通基盤的技術の開発
ものづくり分野・戦略分野における専門職大学院の設置
国際的なビジネス展開・市場拡大のための環境整備
職種別スキル標準の整備等による、人材育成の強化
経営資源の潜在力を引き出すIT活用推進
川上企業・川下企業間のネットワーク構築支援
安全性の確保、PL法上の取扱、各種保険制度等の制度整備
知的資産の評価・管理・活用・開示のための手法作り
国際的な連携強化による、海外リソースの活用
地域独自の戦略に基づく地域基礎力の強化

0% 5% 10% 15% 20% 25% 30%

出典:2010年版 組込みソフトウェア産業実態調査